

ЖУРНАЛ ОТ КОМПЬЮТЕРНЫХ ХУЛИГАНОВ
ХАКЕР
ver 06.03 (54)
WWW.XAKEP.RU
Компьютер будущего:
Что такое нейрокомпьютер и на что он способен
Старший опер Гоблин:
Сделано с особым цинизмом
Открыть ворота!
Связка ключей к мозгу локалки
Хакерские войны:
Legion of Doom vs. Masters of Deception
Почтовые шалости:
Используем недоработки SMTP протокола
Провайдер в домашних условиях
Обзор эксплоитов:
Bysin2 for Sendmail
0x333hate for samba 2.2.x
OpenFuckV2 for OpenSSL v0.9.6d
(game)land
ISSN 1609-1019
9 771609 101009 06>

«Москва» работает и по субботам!

модную **Одежду**
удобную **Обувь**
надежное **Аудио и Видео**
качественную **Бытовую технику**
современные **Компьютеры**
элегантную **Мебель**







54

В середине мая произошло то, чего ждали десятки миллионов: премьера второй части Матрицы. Спецэффекты опять на уровне, но вот сюжет... Господа Вачовски решили, что в первой Матрице не хватало сантиментов, слюней и непонятно-отвлеченной философии. В общем, тошниловка получилась. Меня, честно говоря, и первая часть в идейном плане не очень впечатлила: киберпанку уже столько лет, что его забывать стали. Хотя эффект от фильма все же был: хакеров-новобранцев (готовых спасать планету, естественно) с тех пор заметно прибавилось. Конечно, пока кибергерои отдыхают, попутно занимаясь менее возвышенными делами (думаю, ты понял, какими). Но спасать нас уже давно пора.

И даже не от Матрицы (существуй она на самом деле, разве позволила бы снять про себя такое разоблачающее кино?), которая при теперешнем подходе к развитию хайтека нам не светит еще долго. Спасать от кого? От уродов, которые правят миром? От пузатых магнатов какой бы то ни было индустрии, готовых за очередной миллиард в кармане пойти на любую мерзость (деньги, действительно, портят людей)? От жалких правителей могучих государств, подставляющих свою натренированную задницу по первому зову "средствимущих", сопровождаемому приятным шелестом зелененьких купюр? От ушастых обывателей, озабоченных только своим выживанием в суровых условиях начала третьего тысячелетия (или не озабоченных ничем вообще)? А, может, от самих себя? Ведь именно мы плюем с высокой колокольни на все и вся. Это наше чувство собственного достоинства и значимости опустилось ниже некуда, не позволяя нам делать то, что хотим МЫ, а не дядя Ваня и мистер Джонсон. Это нами вертят, как хотят, все, кому не лень: от создателей тупой рекламы до "советников по госбезопасности", свободно продвигающих идеи тотального контроля над личностью гражданина (пока, правда, только за океаном, но у нас есть все шансы опробовать "зарубежный опыт" на себе). Конечно, жить по принципу "нас ребут, а мы - крепчаем" - тоже выход. А ты не боишься, однажды совсем окрепнув, набравшись сил, сказать свое решительное "НЕТ!" гаду, замочить его в его же собственной уборной и установить СВОИ порядки, обнаружить, что у всей твоей энергии одна судьба - питать ЕЕ. Матрицу... И совсем не обязательно это будет выжившая из своего электронного ума ИИ-машина. И поработившие Землю пришельцы тоже не причем. Но правда всегда где-то рядом. Стоит только насторожиться, посмотреть на вещи под другим углом, и ты поймешь, что ОНА нас уже давно имеет, а мы как бы и не против. Кто ОНА? СИСТЕМА.

Мы все подвластны Ей. Покажи мне человека (которого окружающие не считают психом), делающего что, когда и как он хочет. Таких нет. Все цивилизованные люди - элементы огромной Системы. Она навязывается нам государством (в широком смысле этого слова), религией, общественным мнением, ограничивая самое главное, что у нас есть - Свободу. Причем ограничение это отнюдь не физическое - оно ментальное, в голове. Поэтому самая главная проблема - в нас самих. Как только ты поймешь, что ты - это Ты, жизнь изменится. В какую сторону - зависит ТОЛЬКО от тебя. Весь мир в твоих руках! И нужно-то всего ничего: лишь протянуть их...

AvaLANche

+БРАТСКАЯ МОГИЛА+

/РЕДАКЦИЯ
>Главный редактор
Александр «2poisonS» Сидоровский
(2poisonS@real.xakep.ru)
>Редакторы рубрик
ВЗЛОМ
Иван «CuTTer» Петров
(cutter@real.xakep.ru)
PC_ZONE
Михаил «M.J.Ash» Жигулин
(m.j.ash@real.xakep.ru)
UNIXOID
Артем «Cordex» Нагорский
(cordex@real.xakep.ru)
>Редактор CD
Николай «AvaLANche» Черепанов
(avalanche@real.xakep.ru)
>Литературный редактор
Мария Альдубаева
(litred@real.xakep.ru)

/ART
>Арт-директор
Кирилл Петров «KROt»
(kerel@real.xakep.ru)
Дизайн-студия «100%КПД»

/INET
>WebBoss
Скворцова Алена
(Alyona@real.xakep.ru)
>Редактор сайта
Леонид Боголюбов
(xa@real.xakep.ru)

/PR
>PR менеджер
Губарь Яна
(yana@gameland.ru)

/РЕКЛАМА
>Руководитель отдела
Игорь Пискунов
(igor@gameland.ru)
>Менеджеры отдела
Басова Ольга
(olga@gameland.ru)
Крымова Виктория
(vika@gameland.ru)
Емельянцева Ольга
(olgaeml@gameland.ru)
Рубин Борис
(rubin@gameland.ru)

тел.: (095) 935.70.34
факс: (095) 924.96.94

/PUBLISHING
>Издатель
Сергей Покровский
(pokrovsky@gameland.ru)
>Учредитель
ООО «Гейм Лэнд»
>Директор
Дмитрий Агарунов
(dmitri@gameland.ru)
>Финансовый директор
Борис Скворцов
(boris@gameland.ru)

/ОПТОВАЯ ПРОДАЖА
>Руководитель отдела
Владимир Смирнов
(vladimir@gameland.ru)
>Менеджеры отдела
Андрей Степанов
(andrey@gameland.ru)
Самвел Анташян
(samvel@gameland.ru)

тел.: (095) 935.70.34
факс: (095) 924.96.94

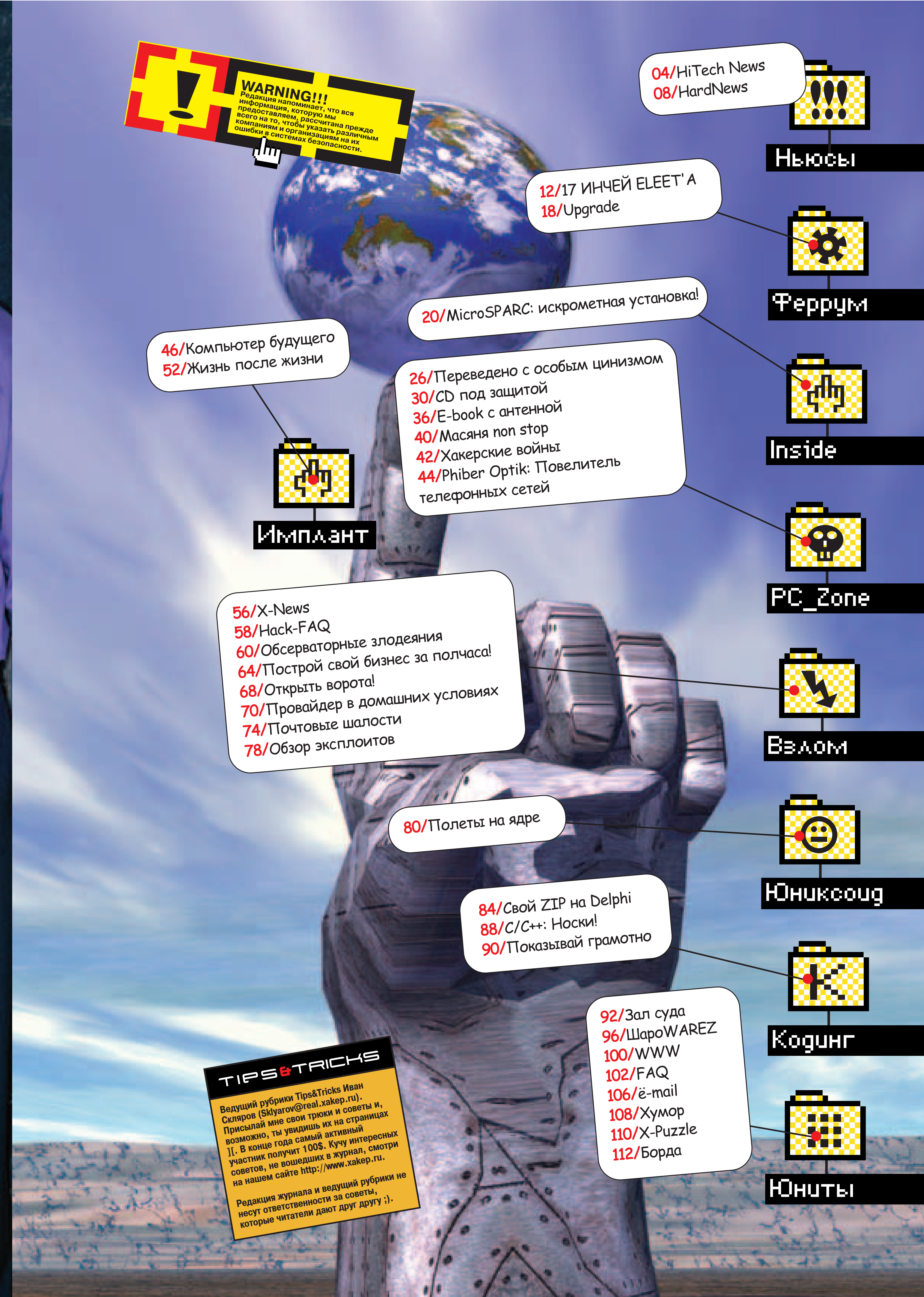
>Технический директор
Сергей Лянге
(serge@gameland.ru)

/ДЛЯ ПИСЕМ
101000, Москва,
Главпочтамт, а/я 652, Хакер
magazine@real.xakep.ru
http://www.xakep.ru

Зарегистрировано
в Министерстве Российской Федерации
по делам печати, телерадиовещанию
и средствам массовых коммуникаций
ПИ № 77-11802
от 14 февраля 2002 г.

Отпечатано в типографии
«**ScanWeb**», Финляндия

Тираж **75 000** экземпляров.
Цена договорная.


WARNING!!!
Редакция напоминает, что вся информация, которую мы предоставляем, рассчитана прежде всего на то, чтобы указать различным компаниям и организациям на их ошибки в системах безопасности.
04/HiTech News
08/HardNews
Ньюсы
12/17 ИНЧЕЙ ELEET'A
18/Upgrade
Феррум
20/MicroSPARC: искрометная установка!
Inside
46/Компьютер будущего
52/Жизнь после жизни
Имплант
26/Переведено с особым цинизмом
30/CD под защитой
36/E-book с антенной
40/Масяня non stop
42/Хакерские войны
44/Phiber Optik: Повелитель телефонных сетей
PC_Zone
56/X-News
58/Hack-FAQ
60/Обсерваторные злодеяния
64/Построй свой бизнес за полчаса!
68/Открыть ворота!
70/Провайдер в домашних условиях
74/Почтовые шалости
78/Обзор эксплоитов
Взлом
80/Полеты на ядре
Юниксоид
84/Свой ZIP на Delphi
88/C/C++: Носки!
90/Показывай грамотно
Кодинг
92/Зал суда
96/ШароWAREZ
100/WWW
102/FAQ
106/ё-mail
108/Хумор
110/X-Puzzle
112/Борда
Юниты
TIPS&TRICKS
Ведущий рубрики Tips&Tricks Иван Скляров (Sklyarov@real.xakep.ru). Присылай мне свои трюки и советы и, возможно, ты увидишь их на страницах][. В конце года самый активный участник получит 100$. Кучу интересных советов, не вошедших в журнал, смотри на нашем сайте http://www.xakep.ru.
Редакция журнала и ведущий рубрики не несут ответственности за советы, которые читатели дают друг другу ;).

!!! Алекс Целых (News@real.xakep.ru)

СТОЛ ДЛЯ ЛЕЖЕБОКИ



■ ErgoQuest (www.ergoquest.com) представила рабочее место для лентяев и лежебок. Конструкция позволяет не просто развалиться в кресле, но пребывать в абсолютно горизонтальном положении. Высота компьютерного стола изменяется в полтора раза, благодаря пневмоподъемнику. Подставка для монитора удерживает его под углом до 60 градусов. Аналогичным образом может варьироваться наклон клавиатуры и "плацдарма" для мыши. Все предметы мебели изготавливаются на заказ в соответствии с пожеланиями клиента. Стоимость новинки - около 3 тысяч "зеленых".

ПРОТЕЗ ДЛЯ СЕЛЕДКИ

■ Ученые, завсегдатаи ресторана в Нью-Йорке, сконструировали инвалидную коляску для золотой рыбки. 17-летний Дик страдает заболеванием плавательного пузыря. Подводная люлька из соломки, марли и ниток позволит рыбке плавать в свое удовольствие, пока болезнь не отступит.

ЭЛЕКТРОННЫЕ МЕМУАРЫ

■ Инженеры British Telecom нашли способ наделять реальные предметы электронными воспоминаниями о прошлом. Морскую раковину, любимого плюшевого мишку или даже пробку от шампанского предварительно помещают в трехмерный сканер. К полученной модели "привязывают" мультимедийную информацию на диске. Когда предмет снова окажется в сканере, и устройство "узнает" его форму, на экране всплывет связанная с предметом история, замелькают фотографии из семейного альбома. Иными словами, вещь расскажет о себе.

САМООБУЧАЮЩАЯ ГИТАРА

■ Yamaha представила самообучающую гитару. EZ-EG помогает постичь азы "семиструнной". Учиться брать аккорды предстоит на псевдострунах. Дюжина светодиодов подскажет правильное положение пальцев на грифе. К 36 обучающим мелодиям можно загрузить дополнительные через порт MIDI. Новинка поддерживает десятки вариантов звучания, включая гитару, бас-гитару, банджо и фортепиано. EZ-EG можно подключить к стандартному гитарному усилителю или использовать наушники для частной практики. Устройство работает от 6 пальчиковых батарей. Продается в интернете по цене 299 долларов.





НЕГОДНЫЕ ПИЛЮЛИ

■ Компания Tacit Technology представила флакон для пилюль, который перестает функционировать по истечении срока годности таблеток. Резьба в новой конструкции не нарезается, а представляет собой отдельную деталь в виде манжеты, которая крепится к горлышку полимерным составом. Со временем это клейкое вещество саморазрушается, после чего крышка прокручивается вхолостую, и ее уже невозможно снять. Срок службы полимерного состава можно запрограммировать с точностью до 1 месяца.

НАБОР РОБИНЗОНА

■ Компания Hammacher Schlemmer представила многофункциональное устройство для настоящих робинзонов. В одном корпусе совмещены сразу 10 приборов, полезность которых на природе не вызывает сомнений. В первую очередь, это пятидюймовый черно-белый телевизор со входом для наушников и складной антенной. Над ним располагается мощный фонарь с ручным фокусом. По бокам - выдвижная флуоресцентная лампа. Две запасные лампочки к ней можно найти во внутреннем отсеке. Кроме того имеются: компас, часы, термометр, сигнальный маяк, сирена, аудиорепеллент от москитов и радиоприемник, настроенный на волну с прогнозом погоды. Устройство весит 1,5 килограмма, работает от блока питания 12 вольт или двух стандартных батареек. Цена в интернете - всего 100 долларов.



ПОТРЕТ БАРАБАНЩИКА

Британские ученые предложили идентифицировать личность по манере человека барабанить пальцами. Новый биометрический датчик нанесен на смарткарту методом трафаретной печати. В основе работы лежат пьезоэлектрические сенсоры, фиксирующие характер постукиваний. По силе и продолжительности удара устройство относит пользователя к тому или иному темпераменту, а затем однозначно идентифицирует личность. При этом система постоянно обучается, занося образцы постукиваний в базу данных. Ученые едины во мнении: на манеру барабанить может повлиять усталость и даже положение пользователя относительно сенсорной панели.

ПЛЕЕР КАЛАШНИКОВА

Компания AudioBooksForFree.com анонсировала MP3-плеер на жестком диске в виде магазина для автомата Калашникова. Конструкция позволяет вставлять устройство на место обычного рожка. Корпус выполнен из нержавеющей стали. Плеер оснащен восьмиминутным антишоком. Емкость диска - 20 Гб, время работы от аккумулятора - 18 часов. Новинку удобно носить в сумке для запасных магазинов к боевому автомату. Ожидаемая цена устройства - около 300 долларов.



ТРЕХГЛАЗЫЙ БИНОКЛЬ

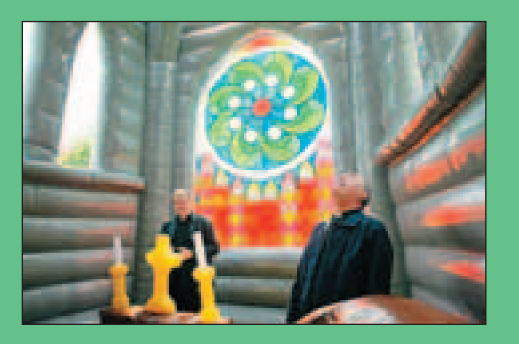
Компания Ezonics представила бинокль со встроенной цифровой камерой. Восьмикратное увеличение EZ BinoCam II гармонично дополняет простенькая камера на CMOS-матрице с автоматическим фокусом и контролем экспозиции. Изображения разрешением до 640x480 пикселов можно хранить на флеш-карте или передать на компьютер через USB-порт. Цена в интернет-магазине - около 60 долларов.



И ЧТЕЦ, И ЖНЕЦ

Компании Toshiba и Matsushita представили интересный гибрид дисплея и сканера. Устройство Input Display внешне ничем не отличается от LCD-экранов карманных компьютеров. Однако, помимо трансляции полноцветной картинки с разрешением 320x240 пикселов, оно способно сканировать в монохромном режиме. Каждый пиксел экрана был усовершенствован крошечным оптическим сенсором. Чтобы ввести изображение предмета в компьютер, следует приложить его к экрану, нажать кнопку и подождать 7 секунд.





НАДУВНАЯ ЦЕРКОВЬ

Первая в мире надувная церковь была освящена в английском городке Эшер. Сооружение в средневековом стиле имеет 14 метров в длину и высоту, 8 метров в ширину и вмещает одновременно до полусотни прихожан. Внутри церкви находятся надувные скамьи, надувной алтарь и даже надувные лампады. Окна набраны пластиковой мозаикой. Надувная церковь чрезвычайно мобильна. В собранном виде она умещается в небольшом фургоне. В рабочее состояние приводится менее чем за 3 часа. Церковь будет служить для заключения помолвок, проведения крестин и брачных церемоний на выезде. Конструкцию можно приобрести в личное пользование за 57 тысяч долларов или взять в аренду за 5 тысяч "зеленых" в сутки.

!!! Алекс Целых (News@real.xakep.ru)

МОТОРИЗОВАННАЯ МЕТЕЛКА 

■ Новосибирские ученые ведут разработку моторизованной метлы. Новинку предполагается оснастить бензиновым или электрическим двигателем. При работе у подъезда метлу можно будет включать в розетку. Всесезонный агрегат призван значительно облегчить труд дворников. При необходимости на метлу навешивается ковш-лопата, рыхлитель льда и другие полезные принадлежности.

СНЕГОДЕЛАТЕЛЬНАЯ МАШИНА 

■ Компания Backyard Blizzard (www.backyardblizzard.com) представила первую в мире машину для производства снега в домашних условиях. Девайс незаменим, если под Новый год хочется лепить снеговика, а погода снежком не балует. Холодильный агрегат на колесах приводится в действие двумя электромоторами. Через садовый шланг организуется подача к машине воды, и уже спустя несколько секунд на землю ложатся первые снежинки. Производительность агрегата - 3 миллиметра снега в час на площади 100 квадратных метров. Рекомендуемая рабочая температура - "минус 3" по Цельсию. Цена - от 1 до 3 тысяч долларов, в зависимости от модели.



КРЫСОБОТ 

■ Ученые Технического университета штата Джорджия представили крысобота - машину, управляемую клетками крысиного мозга. Движения искусственного организма Hybrot контролируют тысячи нейронов, покрывающих 60 электродов на микрочипе. Электрическая активность клеток мозга в реальном времени анализируется на компьютере, который приводит машину в движение. Миниатюрное трехколесное транспортное средство развивает скорость до 1 м/с. Устройство снабжено оптическими сенсорами, которые сообщают его текущие координаты. При пересечении пограничных инфракрасных лучей клетки получают сигнал ретироваться.



НОСОМ ПО ДИСПЛЕЮ 

■ Канадские ученые разработали технику управления курсором при помощи кончика носа. Программное обеспечение "снимает" изображение с веб-камеры, отслеживая малейшие перемещения этой части лица и проецируя их на экран. Необычное устройство ввода уже поддерживает несколько игр. А при помощи редактора Nouse Paint кончиком носа можно рисовать прямо на экране. Нос располагается ближе других частей лица к монитору, поэтому его проще всего распознать.

ТЕЛИК С УШАМИ 

■ Компания Диснея представила серию аудио- и видео-устройств в прикиде Микки Мауса. "Веселая линейка" для детей включает цветной 13-дюймовый телевизор, плееры DVD и компакт-дисков, бумбоксы и портативный радиоприемник. Все устройства имеют простой в освоении интерфейс и другие особенности, характерные для маленьких хозяев. Например, телевизор с отстегивающимися ногами и ушами оснащен "родительской кнопкой" и пультом управления с увеличенными клавишами. В устройства может быть встроена беспроводная Disney-рация для круглосуточных переговоров с родителями. Цена в интернет-магазине - 119 долларов.

ЗАЛ СЛАВЫ РОБОТОВ 

■ Будущей зимой в Американском университете Карнеги-Меллона откроется "Зал славы роботов". Цель акции - отдать дань уважения выдающимся роботам планеты и их гениальным создателям. В экспертную комиссию входят такие монументальные личности, как писатель-фантаст Артур Кларк и директор лаборатории искусственного интеллекта Массачусетского технологического института Родни Брукс. Заявки на включение роботов в экспозицию принимаются до 31 августа 2003 года по адресу james.morris@cmu.edu. Письмо следует сопроводить коротким рассказом, иллюстрациями и видеоматериалами. Роботы-победители в нескольких категориях будут объявлены 30 ноября. Чуть позже представительство музея откроется в интернете.

КАРТОНКА ДЛЯ "МАМЫ" 

■ Lupo (www.lupo.co.jp) и Boxmaster выпустили набор "сделай сам" для сборки системного блока из первосортного картона. На "болванку" нанесены линии сгиба. Перфорацией отмечены отверстия для вентилятора и планок портов. Последние, согласно инструкции, следует аккуратно выдавить. Жесткие диски и съемные устройства перед установкой заключаются в дополнительные кожухи. Диковинный гаджет форм-фактора MicroATX можно приобрести за 80 долларов.

ПОДЗЕМНЫЙ ЗМЕЙ 

■ Японские ученые сконструировали робота-змею, который ведет поиск живых людей под завалами. ACM-R3 состоит из 20 звеньев, связанных в цепь. Встроенные микрофон и камера регистрируют малейшие признаки жизни. Робот способен искать полости и, сгибаясь в суставах, на 6 гусеницах пробираться к жертве сквозь завалы. В сложной ситуации управление роботом по беспроводной связи берет на себя оператор.

GUINNESS ИЗ ГОРЛА 

■ Guinness представляет первое в мире пиво, созданное для того, чтобы пить из горла. В каждую бутылку Guinness Draught встроена специальная капсула "rocket widget" с газом. Как только ты откупориваешь бутылку, гэджет создает плотный слой пены, "фирменной" для бочкового Guinness. При очередном опрокидывании пена снова поднимается до краев, не переливаясь.

Лаконичная форма, **широкие возможности**

BrightWindow

Товар сертифицирован

Новая серия мониторов
LG FLATRON™ ez



Монитор FLATRON™ ez T710P

Трубка	17" FCDT FLATRON™ ez
Точка	0,25/ 0,20мм
Горизонтальная частота	30-85 КГц
Максимальное разрешение	1600x1200 @ 68 Гц
Соответствие стандартам	TCO 99
Дополнительные опции	Bright View/Bright Window

BrightWindow

Эта функция позволяет выделять с помощью мыши интересующий фрагмент изображения и корректировать уровень яркости и контрастности на нём. Также, можно изменять размер окна изображения.

BrightVeiw

Эта функция позволяет выбирать различные режимы из меню в зависимости от того работаете ли Вы с офисными приложениями, растровыми изображениями ил играете в 3D-игры. Каждому из этих режимов предназначен свой уровень яркости от 160 до 350 cd/m^2.

Трубка

Благодаря новейшей электронно-лучевой трубке FCDT, состоящей из плоского экрана и «Маски двойной кривизны» (Double Curved Mask), плоское изображение передается без искажений и смотрится наиболее естественно. В трубке FCDT реализовано несколько новейших разработок LG Electronics: новая электронная пушка iPLS Gun II, обладающая высокой плотностью пучка, как результат, более четкая точка на экране; теневая маска (Ultra Invar) с усиленной структурой.

Цвет

С помощью нового люминофорного покрытия Neo Pigmented Phosphors создаются чистые основные цвета на ярком экране. Это делает изображение более контрастным, с одной стороны, и не утомляющим глаза из-за естественности цветопередачи с другой.

Дизайн

Дизайн новых мониторов отличается привлекательной лаконичностью, удобным расположением кнопок управления, продуманным дружественным интерфейсом, уменьшенной глубиной.



тел.: (095) 777-1044
факс: (095) 958-6019
www.dvm.ru

Москва: Альбино (095) 788-0046, 261-8053; Дилайн (095) 969-2222; Инфорсер (095) 173-9934, 173-9937; Компания MEIJIN (095) 727-1222; Крона Форт (095) 234-0010; НИКС (095) 974-3333; Онлайнтрейд (095) 737-4748, 943-9650; Остров Формоза (095) 926-2452; Систек (095) 781-2384; Стартмастер (095) 967-1515; Техносила (095) 777-8777; Формоза-Полянка (095) 933-4997; Цифровой Мир (095) 785-3888; Электон (095) 956-3819; Forum Computers (095) 707-1306, 707-1309; OLDI (095) 232-3009; Red Diamond Computers (095) 785-8194; ULTRA Computers (095) 729-5244, 729-5255; USN computers (095) 775-8202; **Белгород:** Инфотех (0722) 26-36-18, 26-36-48; **Благовещенск:** Ксерокс-сервис (4162) 44-12-16; **Екатеринбург**: Диджитек (3432) 777-407, 777-408; Ваш компьютер (3432) 711-033, 719-250; **Казань:** Логические Системы (8432) 112233; **Нижневартовск:** Ланкорд (095) 956-05-25; **Пермь:** О-Си-Эс Урал (3422) 195-148 415-441; **Псков:** Компьютерный салон «ВЭБ» (8112) 79-3021; **Ростов-на-Дону:** Компьютер Сити (8632) 72-66-50; Технополис (095) 733-99-49; **Самара:** Крафт-С (8462) 41-2412; Радиант (8462) 34-0706; **Санкт-Петербург:** Альфа (812) 320-80-70; **Смоленск:** Этна Холдинг (0812) 55-8951; **Тольятти:** СофтЭкс (8482) 377-977, 339-515; **Тула:** Курсор (0872) 30-9508; **Тюмень:** Компьютел (3452) 463064; **Уфа:** Форте ВД (3472) 37-9606; **Хабаровск:** Комлэнд (4212) 302-007.



www.lg.ru

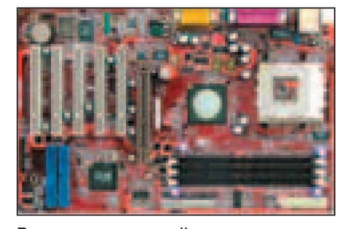
июнь 2003
№54



Оверклокерская мамка

Компания Iwill недавно анонсирована новое семейство материнских плат для платформы AMD K7 - K7S3. Представители этой серии будут работать на базе недавно разработанного чипсета SiS748. Напомню, эта микросхема поддерживает работу с памятью DDR400, а также подразумевает поддержку 400-мегагерцовой процессорной шины. Основные спецификации системной платы:

■ Поддерживаемые процессоры: AMD Duron, Athlon и Athlon XP (разъем Socket 462)
■ Чипсет: связка из микросхем Sis748 и SiS963L, взаимодействие между ними осуществляется при помощи шины MuTIOL на скорости до 1 Гб/сек.
■ Поддерживаемая память: DDR400/333/266/200 (до 3 Гб тремя модулями в слоты DIMM)
■ Шина AGP: поддерживаются режимы 8X/4X
■ Шина PCI: пять 32-разрядных слотов
■ Дополнительные функции:
□ Встроенный 10/100BASE-T Ethernet адаптер на чипе Realtek 8201
□ Интегрированный 5.1-звук (микросхема Realtek ALC650)
□ Шесть(!) портов USB 2.0



Возможность ручной установки частоты системной шины с шагом в 1 МГц, напряжения питания ядра процессора и памяти, а также возможность жесткой фиксации на определенных значениях частот шин AGP/PCI при разгоне - для большей стабильности системы, это оценят бывалые оверклокеры.

Модные USB-часы

Компания Laks представила свою новую разработку - стильные часы, оборудованные встроенной флеш-картой, взаимодействие с которой осуществляется при помощи интерфейса USB 1.1. В настоящий момент в продаже имеется три варианта описываемой модели, различающихся лишь объемом встроенной памяти: 32 портативных мегабайта обойдутся покупателю всего в $50, за 64 Мб производители просят 75 грин, а покупателю самого функционального варианта, оборудованного 128 Мб памяти, придется выложить $105. Доступ к данным осуществляется на скорости порядка



мегабайта в секунду - но это при условии установленной на компьютере ОС Windows, либо Linux с ядром старше 2.4. Не обламываются и владельцы iMac - Mac OS 8.6 и старше без проблем подцепит эту девайсину. Вообще, часики довольно стильные и по внешнему виду догадаться об их скрытых функциях непросто. Устройство оборудовано часовым механизмом от Citizen, системой защиты от статического электричества, ударов и воды (можно нырять на глубину до 20 метров). Весит эта вещица 43 грамма, что, учитывая компактные размеры (11x40 мм), невысокую цену и стильный дизайн, делает ее весьма привлекательной в плане потенциального приобретения.

Милашка от Sony

Компания Sony продолжает линейку своих миниатюрных цифровых камер CyberShot, пополнив ее новой моделью DSC-V1. Эта 5,1-мегапиксельная малышка стоимостью около $850, пожалуй, будет достойным продолжением линейки. Цифровушка оборудована чувствительной 1,8-дюймовой CCD-матрицей, на которой расположено 5,1 млн. эффективных пикселов. Для лучшего восприятия света от фотографируемого объекта применяется отличная оптическая система VarioSonnar, состоящая из восьми линз, две из которых асферические. Камера обладает 4-кратным оптическим зумом, фокусное расстояние от 7 до 28 мм, что в "пленочном" формате составляет 34-136 мм. Камера поддерживает макро-режим, позволяющий фотографировать объекты, находящиеся на расстоянии 8 см от объектива. Для всех цифровых операций применяется 14-разрядный процессор DXP, который руководит всем процессом фотографирования и позволяет пользователю собственноручно устанавливать время, приоритет выдержки и прочее, что заинтересует опытных фотографов. Устройство оборудовано 1,5-дюймовым ЖК-монитором, с помощью которого пользователь



может управлять устройством и просматривать фотографии.
В комплекте с камерой идет 32-мегабайтная карточка Memory Stick, также поддерживаются флешки стандартов Memory Stick Duo и Memory Stick PRO. Помимо фотографий (их максимальный размер составляет 2592x1944), цифровушка может записывать видео в формате MPEG-1 (640x480 @ 17fps). Взаимодействие с компьютером осуществляется при помощи интерфейса USB 2.0. Камера обладает аналоговым TV-выходом, что позволяет демонстрировать фото и видео на большом телевизионном экране.
Весит эта вещица 273 грамма.

Оконный КПК

Корпорация Psion Teklogix начала поставки нового КПК серии 7535, отличающегося наличием хардварной клавиатуры и несколько увеличенным временем работы от аккумуляторов. Технические спецификации новинки:



■ Процессор: 400 МГц XScale PXA 255
■ Память: максимально до 128 Мб SDRAM и 32 Мб Flash ROM
■ Дисплей: 3,8-дюймовый 240x320 мо

Opteron наступает!

Сайт t-break.com опубликовал подробные характеристики новой системной платы для AMD Opteron. На этот раз отличилась ASUStek, выпустив первую маму для Оптерона на базе чипсета от NVIDIA.
SK8N - именно так названа новинка - имеет следующие спецификации:
■ Поддерживаемые процессоры: AMD Opteron (интерфейс Socket 940)
■ Чипсет: NVIDIA nForce3 Pro 150
■ Поддерживаемая память: PC1600/2100/2700 (до 8 Гб четырьмя модулями)
■ Шина AGP: поддерживается режим 8x
■ Дополнительные функции:
- 2 канала ATA-133
- 2 порта Serial ATA-150
- 6 портов USB 2.0
- Поддержка шины FireWire
- Интегрированный Ethernet-адаптер 10(100)BASE-T (чип RTL8201BL PHY)

- Интегрированный 5.1-звуковой адаптер, базирующийся на кодеке AC'97
- Поддерживаются также все фирменные технологий ASUS (ASUS MyLogo2, ASUS EZ Flash, ASUS C.P.R.(CPU Parameter Recall), ASUS CrashFree-BIOS, ASUS Q-Fan, ASUS Multi-language BIOS, etc), что подразумевает возможность оверклокинга систем, базирующихся на этой платформе.

И в огне не горит!

Panasonic на днях представил общественности новый пылевлагозащищенный ноутбук на интеловской плат-



форме Centrino. Toughbook CF-73 построен на базе процессора Intel Pentium M, работающего на частоте 1,4 гигагерца и оснащенного одним мегабайтом кэш-памяти второго уровня. Кристалл работает с системной шиной на частоте в 400 мегагерц, оснащен 13,3-дюймовым TFT ЖК-дисплеем, 256 мегабайтами памяти DDR RAM, видеоадаптером ATi Mobility Radeon 7500 (подключается к шине AGP с поддержкой режима 4x), 40-гигабайтовым жестким диском UltraATA100 и DVD/CDR-W-приводом. Помимо стандартного 802.11 - адаптера и Bluetooth, в CF-73 встраивается, по желанию и возможностям клиента, CDMA или GPRS-модем. Также имеется два разъема PCMCIA (в т.ч. с поддержкой SmartCard), mini-PCI и интерфейс USB 2.0. Ноутбук оборудован 56K-модемом, 100(10)BASE-T Ethernet-адаптером. Стандартный аккумулятор устройства обеспечивает емкость 3,8 А/ч, чего, по утверждениям разработчиков, достаточно для автономной работы в течение пяти с половиной часов.

Мама для P4

Компания SuperMicro, специализирующаяся преимущественно в области разработки серверных решений на платформе Intel, представила две новые системные платы собственного производства. Выпущенные новинки работают на базе чипсета Intel 865G/PE: P4SPA+ и P4SPE. Платы поддерживают 400-мегагерцовую системную шину, 8x-режим шины AGP, на обеих платах размещена звуковая карта и сетевой адаптер.
Основные характеристики новинок:

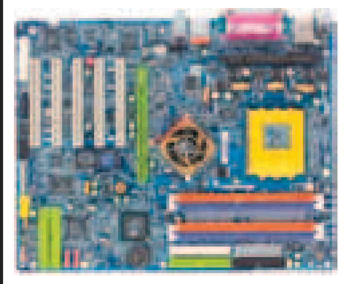


■ Поддерживаемые процессоры: Intel Pentium 4 и Intel Celeron с тактовой частотой до 3,06 ГГц, системной шиной 800/533/400 МГц и технологией Hyper Threading.
■ Чипсет: Intel 865G/PE
■ Поддерживаемая память: двухканальная DDR400/333/266 SDRAM (до 4 Гб четырьмя модулями)
■ Шина AGP: поддерживается режим 8x
■ Шина PCI: пять 32-разрядных слотов расширения
■ Дополнительные функции: встроенный 100(10)BASE-T Ethernet адаптер, два порта SATA, интегрированная видеокарта Intel EXTREME GRAPHICS II (в P4SPA+), восемь(!) портов USB 2.0, встроенный 5.1 звуковой адаптер на базе кодека AC'97.

Супермама

Компания Gigabyte Technology представила новую модель из линейки платформ на базе чипсета NVIDIA nForce2, выпуск которого связан с появлением процессора AMD Athlon XP, работающего на 400-мегагерцовой системной шине.

В основе системной платы GA-7NNXP лежат компоненты суперсовременного чипсета NVIDIA nForce2 Ultra 400 System Platform Processor (SPP), поддерживающего следующие технологии: Dual Power System (DPS), Dual LAN, Dual Channel DDR, Dual Cooling System, Dual RAID, DualBIOS.
Основные технические характеристики платы GA-7NNXP:



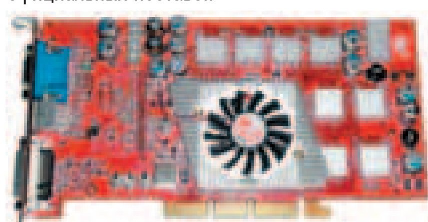
■ Поддерживаемые процессоры: AMD Athlon XP с 400 МГц системной шиной
■ Чипсет: NVIDIA nForce2 Ultra 400 SPP + MCP-T
■ Шина AGP: поддерживается режим 8x
■ Шина PCI: пять 32-разрядных слотов расширения
■ Поддерживаемая память: Двухканальная DDR 400/333 (до 3 Гб четырьмя модулями DIMM)
Плата поддерживает технологию Dual Power System с Dual Power Voltage Regulator Module, оборудована 1000BASE-T Ethernet адаптером на базе чипа Intel 82540EM, имеет IDE RAID-контроллер ITE GigaRAID, 3 порта IEEE1394, 6 портов USB 2.0 и интегрированный 5.1 звук на базе кодека AC'97.



июнь 2003
№54

Опасайся: видеомонстры!

На сайте компании ATI Technologies недавно появился пресс-релиз, в котором представители компании извещают общественность о начале официальных поставок



новых графических адаптеров RADEON 9800 PRO. Новинка оборудована 256 мегабайтами памяти DDR-II, которая работает на частоте в 350 мегагерц. Процессор устройства совершает 380 миллионов тактов в секунду, что в совокупности с 256-разрядной шиной памяти обеспечивает недетскую производительность.
Чип видеокарты оборудован алюминиевым радиатором и собственным вентилятором, кроме того, для более эффективного охлаждения устройства, на каждой микросхеме памяти находится собственный радиатор.
В пресс-релизе также говорится, что карты RADEON 9800 PRO 256MB поставляются в ограниченном количестве, а рекомендованная розничная цена новинки - $499.

Новый плеер от Thomson

Фирма Thomson пополнила линейку цифровых плееров Lyra, представив на днях новые модели: PDP 2424 и PDP 2428. Карманный цифровой плеер PDP 2424 воспроизводит форматы MP3 и WMA и оснащен не только встроенной флешкой объемом 64 Мб, но и



интерфейсом для подключения дополнительных карт памяти. В комплекте с устройством идет компьютерная программа MusicMatch, позволяющая пользователю быстро создавать и редактировать свои собственные музыкальные коллекции. Взаимодействие с компьютером осуществляется через USB-порт, что позволяет быстро закачивать музыку в плеер. Плеер оборудован большим жидкокристаллическим дисплеем, на котором отображается информация о проигрываемых композициях. Плеер стильно смотрится и имеет небольшие размеры: 62x62x20 мм, весит устройство 80 граммов. Основное отличие модели PDP 2428 заключается в увеличенном объеме флеш-памяти, емкость которой в этой модели составляет 128 Мб.

ParaDIGMus-2003

В конце июня ты сможешь побывать на самой настоящей демо-пати. Сценерская туса состоится под Москвой, в славном городе Серпухове. Номинации (PC и ZX Spectrum):
- **PC DEMO,**
- **PC GRAPHICS,**
- **PC MUSIC,**
- **Rendered ANIMATION,**
- **FLASH ANIMATION**
- **ZX DEMO,**
- **ZX GRAPHICS,**
- **ZX AY MUSIC**
- **WILD COMPO**

Чтобы приобщиться с ELEET'ной демосценерской культуре, надо всего лишь с утречка 28-го июня отбыть на электричке с Курского вокзала или на автобусе от м. Южная в направлении Серпухова (ул. Фирсова, д.5, Московский областной педаго-



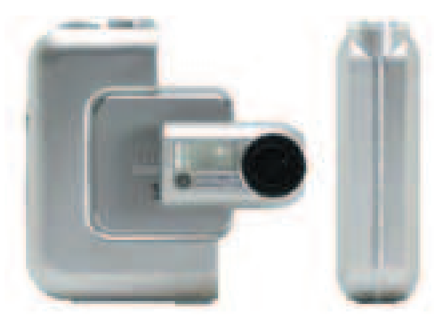
гический колледж) и в 11.00 быть на месте. Кстати, ты сможешь выступить и в качестве участника, если привезешь с собой свое нетленное демотворчество. Увидимся на ParaDIGMus'е!

SMC проставила маршруты

Компания SMC Networks начала поставки двух новых четырехпортовых маршрутизаторов, оборудованных встроенными ADSL-модемами (это SMC7404BRA и его беспроводная вариация SMC7404WBRA). Новинки продолжают линейку Barricade и ориентированы на рынок сетевого оборудования, используемого в небольших офисных сетях.
Как уже отмечалось, обе модели имеют встроенный ADSL-модем. Новинки также имеют по четыре Ethernet 100(10)BASE-T порта для подключения к локальным сетям с пользователями, пакеты которых либо роутятся, либо натятся (в случае использования внутренней адресации) в инет. Беспроводная SMC7404WBRA также обладает точкой доступа IEEE 802.11b 11 Мбит/с для подключения удаленных радиоклиентов.
Обе модели могут выступать в качестве DHCP-сервера и автоматически раздавать IP клиентам при входе в сеть. Само собой, возможен хитрый роутинг и натинг пакетов между всеми четырьмя сетями, с поддержкой технологии Stateful Packet Inspection.
Присутствует возможность организации VPN-туннелинга в интернет и любую локальную сеть.
Конфигурация устройства выполняется удаленно при помощи любого браузера в операционной системе, поддерживающей протокол TCP/IP.

Поворотный момент Nikon

Фирма Nikon начинает официальные поставки в Россию своей новой 3,1-мегапиксельной камеры COOLPIX SQ. Новинка выгодно отличается совершенной оптикой, позволяющей снимать объекты, находящиеся на расстоянии в несколько сантиметров от объектива. По словам разработчиков, существенное внимание было уделено и цветопередаче: сверхчувствительная 3,1-мегапиксельная матрица позволяет достичь отличного качества снимков без ручной цветокоррекции. Кроме того, устройство поддерживает множество сценариев работы для различных условий (яркое освещение на снегу, слабое в сумерках, съемка в движении и т.д.), что позволяет делать снимки еще более качественными. Устройство также отличается высокой скоростью работы - характерные задержки при включении здесь сведены к минимуму, и у тебя есть шанс успеть "поймать" ценный кадр. Основные спецификации устройства:





- Матрица: 1/2,7" 3,1 эффективных мегапикселов
Размер изображений: до 2016x1512
- Объектив: 3-кратный Zoom-Nikkor; f=5,6-16,8 мм (соответствует для 35 мм формата 37-111 мм) F2,7-4,8; Цифровой зум: до x4.0
- ЖКИ монитор 1,5"; 117,600 точек, трансфлективный TFT ЖКИ-монитор на низкотемпературном поликремнии с регулировкой яркости
- Носитель данных: карточки памяти CompactFlash(tm) (CF) тип I
- Режимы съемки: автоматический, 15 сюжетных режимов, видео (видеоролики до 40 сек 640x480 @ 14 fps со звуковой дорожкой)
- Встроенная вспышка: съемка на расстоянии 0,15-5,0 м (W); система управления вспышкой с датчиком; режимы вспышки: Auto, Отключение вспышки (выкл), Подавление эффекта "красных глаз", Принудительная вспышка
- Источники питания: интегрированная литий-ионная аккумуляторная батарея EN-EL2, сетевой блок питания EH-61
- Ресурс батареи: около 65 мин непрерывной съемки для EN-EL2 с использованием ЖКИ монитора
- Размеры: 82x82x25,5 мм
- Вес: 180 г

Особо хочется отметить внешний вид новинки - стильный металлический корпус в сочетании с необычными формами придает камере неповторимую изюминку.



test_lab (test_lab@gameland.ru)

17 ИНЧЕЙ ELEET'A

тестирование LCD-мониторов

322

Самый актуальный размер монитора на сегодня — это 17 дюймов, а самая актуальная технология — LCD. Так что тест семнадцатидюймовых плоских мониторов по дефолту становится актуальнее всех остальных мониторных тестирований. Вывод: в этом номере у нас самый главный тест мониторов за год. Читай внимательно — не пропусти!

К основному 31337-тесту мониторов мы готовились долго, и подошли к вопросу основательно. Для проведения субъективных тестов мы подключали сразу несколько мониторов к одной видеокарте через VGA-разветвитель (VGA-splitter). Таким образом можно было сравнить мониторы на одном и том же тестовом изображении. Перед сравнением мониторы настраивались на оптимальное отображение. Во время тестирования мы заюзали профессиональный колориметр. Этот прибор используется для проверки основных характеристик изображения монитора, таких как цветопередача, яркость изображения, нелинейность, дискретность, неравномерность спектра. С его помощью проводят очень точную калибровку мониторов, это в первую очередь необходимо тем, кто работает с графикой и цветом. После калибровки прибор создает профиль монитора (для Windows) со всеми необходимыми исправлениями. Для теста же важно то, что колориметр позволил нам оценить качество изображения не только визуально (субъективно), а еще программно-аппаратно, а значит точно.

В отличие от качества изображения, дизайну каждого монитора мы дали субъективную оценку, при этом учитывали не только внешний вид, но и удобство использования. Самым симпатичным был признан Viewsonic :). Монитор SAMSUNG SyncMaster 171P умеет переворачиваться в портретный режим, что делает удобным просмотр фотографий и текстов на странице формата A4. На экране помещается страничка целиком. Также мы считаем очень удобным размещение блока питания в корпусе монитора, этим отличились CTX, HYUNDAI и PHILIPS. Наличие большого количества проводов и лишних предметов на рабочем месте бесит, так что внешний блок питания хотя и имеет свои плюсы, но, в конечном счете, является минусом :).

Дальше мы перечислим и опишем все те свойства LCD-мониторов, которые мы считаем важными. Все мониторы тестировались с учетом этих пунктов. Некоторые свойства выведены в таблички, чтоб тебе удобнее было их воспринимать, а о некоторых мы упомянули прямо в описании к конкретному монитору.

ЭНЕРГОПОТРЕБЛЕНИЕ

Плюсом LCD-моников принято считать низкое энергопотребление. CRT'шки едят электричества примерно в два раза больше. По паспортным данным наименее прожорливым оказался CTX, хотя по нашим впечатлениям он грелся больше всех.

ЯРКОСТЬ И КОНТРАСТНОСТЬ

На графике отложены паспортные данные по яркости и контрастности. Яркость измеряется в канделах на квадратный метр. Она зависит от мощности ламп подсветки и от способности жидких кристаллов пропускать свет без потерь. Контрастность показывает, во сколько раз отличается самая яркая точка от самой темной точки, которую способен высветить монитор.

УГЛЫ ОБЗОРА

Существенный минус LCD-мониторов - ограниченный угол, под которым можно нормально разглядеть изображение. Если смотреть на LCD-дисплей под углом, то в зависимости от угла будут меняться яркость, контраст, цвета. Мы построили графики по паспортным данным мониторов.

МЕРЦАНИЯ И ПЕРЕЛИВЫ

Многие наивно полагают, что от LCD-монитора не устают глаза, но это совсем не так. Начнем с того, что от длительного чтения обычного текста или от длительного рассматривания вообще чего-либо глаза устают! Основная причина усталости глаз при работе за CRT-монитором - мерцание изображения. Однако на частотах развертки 85-100 герц этот эффект сильно снижается. LCD-дисплей не мерцает вообще. Зато он переливается, и от этого тоже устают глаза. Дело в том, что человек постоянно двигает глазами и головой при работе за компьютером, и из-за этого изображение переливается. Многие перцы, проводящие весь рабочий день в офисе за ЖК-монитором, жалуются, что их утомляет этот эффект. Хотя есть и те, которым переливы нравятся больше, чем мерцания. Также глаза могут уставать от нечеткого, темного, расплывчатого изображения, то есть от некачественного LCD или CRT-монитора.

ФОКУСИРОВКА И ТИП ИНТЕРФЕЙСА

На CRT-мониторе под фокусировкой электронного пучка можно понимать радиус зайчика на экране, который он отбрасывает. То есть размер точки. Если точки будут жирными, то и фокус будет размытый. Большая проблема CRT - неравномерность фокусировки, то есть в одном месте экрана фокус может быть четким, а по краям размытый. У LCD-дисплеев фокус должен быть идеальным, так как все ячейки матрицы одного размера, и каждая на своем месте. Но и на ЭЛТ-мониторе могут быть неравномерные замыливания изображения, похожие на проблемы с фокусом.

АНАЛОГОВЫЙ ИНТЕРФЕЙС

Обычно видеокарта преобразует цифровой сигнал в аналоговый: три цвета и синхронизация. Для электроннолучевого монитора этот сигнал удобен, так как изображение формируется плавными изменениями напряжения на электронных пушках и на катушках отклонения. То есть электроннолучевая трубка управляется аналоговыми сигналами. Матрица LCD-дисплея - цифровое устройство, самый настоящий массив точек. Поэтому аналоговый сигнал с адаптера приходится преобразовывать в цифровой. Во время этого преобразования изображение может ухудшаться, в результате появляются замыленности. Чтобы привести изображение в норму, монитор должен автоматически настроить свой аналого-цифровой преобразователь.

ЦИФРОВОЙ ИНТЕРФЕЙС

Качество изображения в этом случае лучше, так как гимор с преобразованием цифра-аналог-цифра отпадает. В LCD-монитор через такой интерфейс поступает удобный для него цифровой сигнал. К сожалению, такие интерфейсы есть не на всех мониторах, и мы считаем это большим минусом. Спрашивается, зачем покупать дорогой LCD-мо-

нитор, чтобы маяться с отмирающим уже аналоговым гимором? Тем более что большинство современных видюх имеют два типа интерфейса: аналоговый и цифровой.

ЗАПАЗДЫВАНИЕ МАТРИЦЫ

Каждая точка TFT-матрицы хранит свое состояние до прихода нового сигнала об изменении. Поэтому LCD не мерцает. Если на CRT-мониторе одновременно горит только одна точка - зайчик луча, то на ЖК все точки горят одновременно. Глаз человека очень инертен, поэтому если зайчик пробегает экран 85-100 раз в секунду, то кажется, что весь экран заполнен точками, а мерцание незаметно.

Но не забывай, что на переключение каждой ячейки TFT-матрицы требуется время. Все мониторы из нашего теста дают очень хорошие результаты по запаздыванию матрицы, сравнимые с CRT. Проверить скорость реакции матрицы легко, для этого загрузи в Word любой текст и быстро прокрутите. Если запаздывание у монитора большое, текст смажется. Кстати, у CRT также можно наблюдать запаздывание: для этого проведи быстро белым курсором мыши по темному экрану, и ты увидишь белый шлейф. Это инертный люминофор не успевает гаснуть ;). У LCD обратная болезнь - точки не успевают зажигаться.

ГЕОМЕТРИЯ

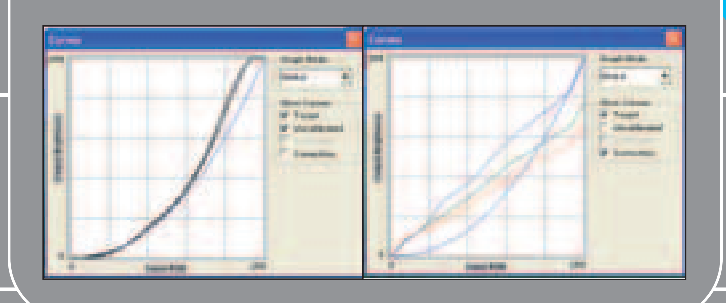
Под геометрией понимают способность дисплея рисовать круги круглыми, а не овальными, прямые линии прямо, а не криво. То есть способность избегать геометрических искажений. У ЭЛТ-дисплеев с геометрией традиционно очень большие проблемы. На изображение ЭЛТ-монитора влияет кривизна экрана, бочкообразные, трапецидальные, сдвиговые искажения. Проблема в том, что пучком электронов довольно сложно управлять точно. Точка, которую выбивает электронный пучок на люминесцирующем слое, может гулять в зависимости от различных обстоятельств. На матрице ЖК-дисплея каждая точка на своем постоянном месте, потому геометрия соблюдается отлично. Но все равно нет ничего идеального на свете: LCD также имеют еле заметные искажения на левой и правой границе матрицы.

SAMSUNG SYNCMASTER 171P



Samsung SyncMaster 171P порадовал привлекательным внешним видом, и это неудивительно, ведь дизайн монитора разрабатывался компанией Porsche. Вообще, этот монитор можно очень легко настроить "под себя", так как он имеет четыре степени свободы. Экран поворачивается на 90 градусов (портретный режим), благодаря чему на экране можно уместить целый лист формата A4. Это очень удобно при серфинге Сети, при подготовке документов и т.д. У монитора имеется удобная вращающаяся подставка и ручка для переноски. Кнопочки управления на лицевой стороне девайса выполнены в виде сенсорной панели, с одной стороны это удобно, так как кнопки почти не пачкаются и чистить их легко, с другой стороны - они слишком чувствительные, и расположены очень близко друг к другу, поэтому есть небольшая вероятность нажать не ту кнопку.

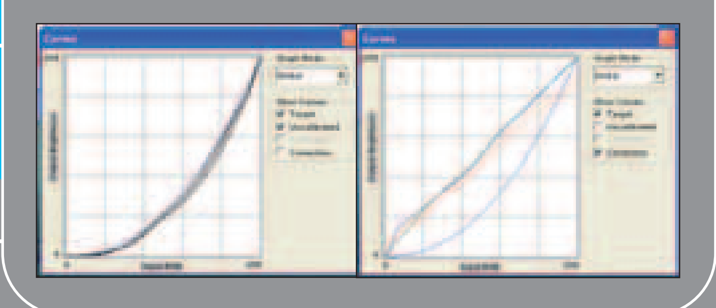
Монитор оснащен входами D-SUB и DVI. По техническим характеристикам Samsung SyncMaster 171P - один из самых ярких и контрастных. При этом имеет неплохой график цветопередачи, он достаточно линеен. В некорректированном виде колориметр не справляется, поскольку рассчитан на 200 кд/м2, а монитор дает 250 кд/м2. Именно поэтому на графике кажется, что монитор заваливает на большой яркости цвета, но на самом деле это не так. Фотографии выглядят довольно естественно. Но самый лучший эффект достигается в играх - за счет соотношения яркости и контрастности хорошо видны детали как в темных, так и в светлых местах. То есть ты можешь шлепнуть сетевого врага, даже если он прячется далеко в тени. Цифровой вход DVI позволяет избежать традиционных проблем с четкостью картинки.



CTX S700



Этот монитор показал себя весьма разносторонне. С одной стороны очень хорошее качество картинки, что в принципе неудивительно, а с другой - слабый, очень простой, даже можно сказать примитивный дизайн и не очень удобное меню, хотя панель управления у него нормальная, кнопки достаточно большие, расположены удобно, случайное нажатие на соседнюю кнопку во время настройки монитора практически исключено. Основным недостатком данного монитора является то, что у него нет DVI-входа, ведь при подключении LCD-монитора через этот вход качество картинки поднимается на несколько порядков, а стандартный D-SUB не снимается, что не очень удобно. У монитора внутренний блок питания, с одной стороны это его плюс, но с другой стороны - если блок питания не очень качественный, он будет греться, а это уже плохо. На графике видно, что на максимальной яркости и контрастности (яркость 250 кд/м2, контрастность 350:1) монитор цвета не заваливает, а после коррекции качество становится еще лучше. Изображения выглядят вполне естественно, никаких искажений нет, в играх тоже все хорошо, все детали видны. У монитора очень хорошая цветопередача, но слабоватая контрастность, если выкрутить яркость и контрастность на максимум, на экране становится виден легкий туман.



test_lab выражает благодарность за предоставленное оборудование компаниям "ОЛДИ" (105-0700), "Сетевая Лаборатория" (500-0305) и "Остров Формоза" (926-2452).

NEXT

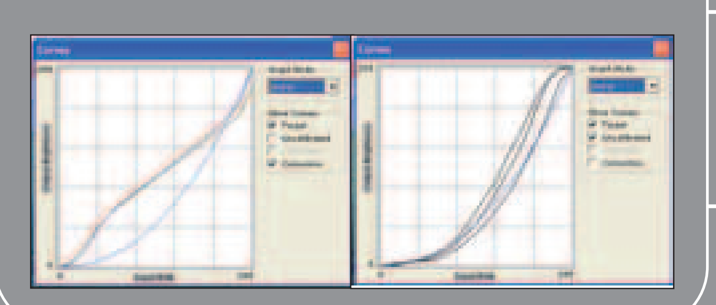




IIYAMA AS4314UT



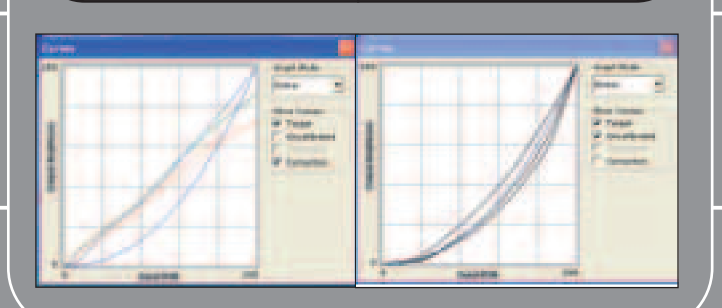
Iiyama as4314ut имеет очень неплохой эргономичный дизайн, меню вполне удобное, панель управления тоже. Теперь недостатки: у девайса нет DVI-входа, а D-SUB несъемный (съемный намного лучше, так как в случае, если шнур переломится, или отвалится контакт в разъеме, его можно просто поменять, а когда такая проблема возникает с несъемным, то придется везти монитор в ремонт, а он стоит немалых денег), блок питания внешний, о достоинствах и недостатках этого уже было написано выше, что лучше - решать покупателю. Яркость монитора 250 кд/м, контрастность 500:1, параметры лучше, чем у CTX S700, но все же хуже, чем у Samsung 171P. После тестирования колориметром выяснилось, что монитор завалил два цвета: это было хорошо видно при вывернутых до конца яркости и контрастности, и так же хорошо видно на графике. Во многих местах игры были замечены неестественные светлые участки, а облака на рабочем столе Windows потеряли оттенки и стали белыми, из этого можно сделать вывод, что монитор не очень качественный, что довольно странно, ведь компания Iiyama делает очень хорошие мониторы. Возможно, нам просто попался неудачный экземпляр. После коррекции профиля монитора с помощью колориметра положение стало намного лучше, но фотографии все равно выглядели не очень естественно (особенно лицо человека, сфотографированное с большим разрешением), зато существенно улучшилось положение в игре, светлых пятен почти не было видно.



VIEWSONIC VE700

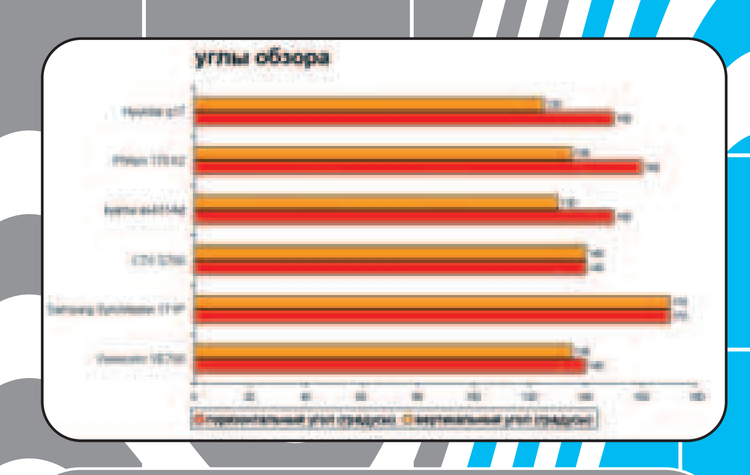


Дизайн монитора классный, он будет прекрасно смотреться в любой обстановке, с этим проблем у компании вроде никогда не было. Меню хорошо продуманное и удобное, кнопки большие, нажимаются легко и расположены достаточно далеко друг от друга. Вообще, стоит отметить такую вещь, как количество кнопок на панели управления - чем их меньше, тем удобнее лазить по меню монитора. Когда кнопок слишком много, управление получается запутанным, и есть большая вероятность нажать что-нибудь не то. Питание у монитора внешнее, провод D-SUB съемный - в случае чего можно легко поменять, благо стоит он недорого. DVI-входа у монитора не предусмотрено, это его главный минус. Тестирование показало, что монитор прекрасно отображает цвета, в этом отношении к нему претензий нет. На максимально яркости и контрастности цвета не заваливает, лица на фотографиях выглядят вполне естественно, игра тоже не выявила никаких дефектов - картинка отображается ярко и четко, все детали прекрасно видны. После коррекции изображение стало еще лучше. В общем, монитор получился очень хороший, если бы не одно "но", а именно отсутствие DVI, вот с этим компания-производитель сильно прогадала. Если бы не это, монитор составил бы достойную конкуренцию Samsung SyncMaster 171P, но, видно, не судьба :).



17 ИНЧЕЙ ELEET'A

test_lab (test_lab@gameland.ru)

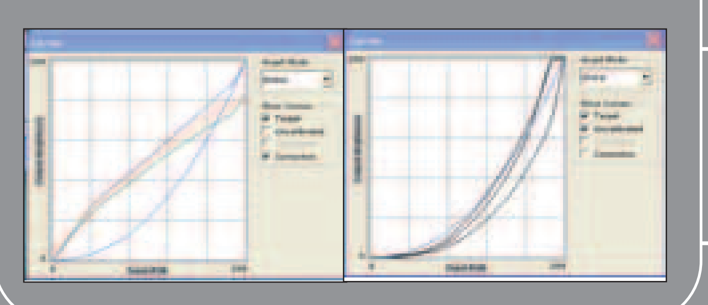




PHILIPS 170 B2



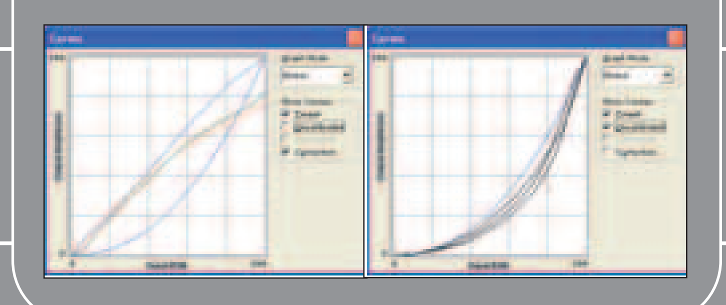
Единственный монитор в тестировании, выполненный в темно-сером корпусе, на наш взгляд такой корпус наиболее практичен, так как на нем совершенно не видны пыль и пролитое пиво :). Дизайн монитора очень приятный и отлично дополнит кузов системника черного или серого цвета. Панель управления средненькая, выглядит она неплохо, но пользоваться ей не очень удобно. Кнопки слишком маленькие и жесткие, нажимать их неподручно. Меню простое и понятное, с этим проблем нет. Вообще, корпус монитора продуман неплохо, все кабели отключаются, предусмотрены как D-SUB, так и DVI-входы, что, безусловно, большой плюс. Блок питания внутренний, и что самое интересное в этом мониторе - возможность питания монитора от внешнего 12-вольтового источника. Можно придумать много применений этой особенности. Например, его можно прикрутить к торпеде (в машине) и, подключив к ноутбуку, смотреть в дороге фильмы =). Однако тестирование показало, что с изображением не все так хорошо, как хотелось бы. На максимальной яркости и контрастности монитор завалил два цвета, естественно, это довольно сильно сказалось на изображении, в игре наблюдались все те же светлые пятна, а на лице (на фотографии) стала видна оранжевая "сыпь", да и кожа выглядела как искусственная. Облака на рабочем столе тоже "побелели". После коррекции с помощью колориметра все встало на свои места, и картинка стала выглядеть намного естественнее. Хочется верить, что в низких результатах виноват именно данный экземпляр, ведь монитор очень неплохо продуман и собран, и если бы не этот дефект, имел бы большие шансы на победу.



HYUNDAI Q17



Монитор имеет простой, но приятный дизайн. Создается впечатление, что он проектировался для использования в серьезном офисе - такой строгий и без излишеств. Кнопки тонкие и длинные, но, как ни странно, довольно удобные, меню тоже простое и удобное, никаких проблем нет. Единственная проблема, относящаяся не только к этому монитору, но и к большинству других в тестировании, состоит в том, что большинство производителей до сих пор не знают, что есть такая страна - Россия, и что там говорят на русском языке. Поэтому в меню можно встретить любой язык, вплоть до каких-нибудь африканских наречий, но русского точно не будет. Hyundai q17 очень хорошо продуман, все провода отключаются, вделанных намертво в монитор нет. Имеется D-SUB и DVI, блок питания внутренний, в подставку монитора вмонтирован USB-хаб, разъем для колонок (в корпусе с обратной стороны экрана вмонтированы 2-ваттные стереоколонки) и разъем для наушников. Это очень удобно, особенно если монитор будет использоваться в офисе, т.к. во время работы можно, никому не мешая, послушать музыку. Тест показал, что на максимальной яркости и контрастности монитор демонстрирует великолепную картинку, не заваливая при этом ни одного цвета. Фотография выглядит очень реалистично, а в играх нет никаких светлых пятен, и четко видны как темные, так и светлые детали. Коррекция цветов не дала существенных результатов, так как изображение было хорошим и до этого.



ВЫВОДЫ

В нашем тестировании безусловным победителем является монитор Samsung SyncMaster 171P, Мы бы выбрали для себя этот монитор, т.к. он обладает хорошей яркостью и контрастностью, очень хорошо передает цвета, у него самый большой угол обзора, есть DVI, его конструкция очень хорошо продуманна. Монитор Hyundai q17 заслужил второе место, его характеристики скромнее, но результат он показал близкий к победителю. Остальные мониторы в нашем тестировании либо имели хорошее качество изображения, но не имели DVI-входа, либо наоборот.

AMD ATHLON XP 2500 - (BARTON)

СУПЕР ВЕЩЬ!

Для демонстрации преимуществ рекомендуемого нами камня мы прогнали его по нескольким стандартным тестам. Старый добрый Q3 отражает картину лучше всего :). Для сравнения был взят Intel Pentium 4 2800Mhz. AMD'шный же проц прогонялся через тесты дважды: в разогнанном и в неразогнанном состоянии.

Quake III Team Arena, MPdemo1

	1024X768 (HQ)	640X480 (Fastest)
AMD Athlon XP 2800+ (разгон)	169.5	241.2
Pentium 4 2800 Mhz	156.7	244.3
AMD Athlon XP 2500+	152.8	233.6

Athlon XP 2500+ - это младшая модель в линейке AMD Athlon XP на ядре Barton. Для настоящих фанатов, которым не терпится проверить возможности нового ядра и при этом отвалить не больше 100-150 зеленых президентов, это фишак. Сам посуди, топовые камни из той же линейки стоят пока что как минимум в полтора раза дороже: Athlon XP 2800+ - 224 космокредa, Athlon XP 3000+ - 324 космокреда и Athlon XP 3200+ - 464 космокреда. Кроме того, факт, что модель является младшей в линейке, сам по себе говорит о невероятных возможностях по разгону. Так уж повелось у разработчиков железа, что младшие модели часто переделываются из старших путем искусственного понижения их рабочих характеристик. Соответственно, если потом их кто-то искусственно повышает ;), результат достигается весьма неплохой.

Мы проверили - камень действительно отлично гонится! Теоретически можно получить рейтинг 3200+, мы же разогнали до 2800+ совершенно без напрягов. Ты только подумай, экономится около сотни зеленых президентов!

Основное отличие ядра Barton от Thoroughbred - это 512 Кб кэша. Оба кристалла изготовлены по технологии 0,13 микрон. Минимальный литографический размер определяет размер всех элементов на кристалле, а значит задержки распространения сигнала, максимальную частоту работы процессора, тепловыделение. Если не считать дополнительный КЭШ, который удлиняет кристалл, то визуально ядра практически идентичны. Однако новые частоты не даются так просто, скорее всего, компания AMD серьезно поработала над технологией производства новых кристаллов. Возможно, были лучше проработаны цепи, улучшены электрические характеристики вентилей.

КАКУЮ МАМКУ ВЫБРАТЬ?

Многие юзеры стоят перед проблемой выбора материнской платы, совместимой с процессором AMD Athlon XP, или не знают, будет ли работать уже имеющаяся мать с новым процессором. Все материнские платы, сделанные на основе чипсета VIA KT333, поддерживают ядро Thoroughbred; не стоит отказываться и от VIA KT266A. Все же мы рекомендуем перестраховаться, посетив сайт производителя, и при необходимости скачать свежую версию BIOS. Что касается поддержки ядра Barton и, следовательно, частоты системной шины в 333 МГц, то таковой обладают следующие чипсеты: VIA KT333, VIA KT400, VIA KT400A и NVIDIA nForce2.

Тут есть еще одна тонкость. AMD официально разрешит только те мамы, которые поддерживают технологию System Bus Disconnect. Благодаря этой технологии процессор AMD будет отключаться от шины на время простоев. То есть переходить в высокоимпедансный режим входов (Z). Также Idle-режим позволит защитить процессор от перегрева. Представители AMD заявляют, что теперь с работающего камня можно снимать кулер. Главное, чтобы системная плата поддерживала спящий режим процессора. Кстати, благодаря этому режиму и вентилятору с переменной частотой вращения, можно будет сделать комп потише.

Из широкого выбора материнских плат хотелось бы выделить продукцию компаний ASUS, ABIT, MSI, EPOX и SOLTEK, уже давно пользующихся популярностью на рынке. Помимо прочего, эти производители предоставляют удобные средства для разгона системы, максимально упрощая пользователям задачу. Особенно успешна в этой области компания EPOX со своими материнскими платами EPOX 8K9A2(+) и EPOX 8RDA(+), которые дают возможность менять заблокированный множитель процессора. Без какого-либо увеличения напряжения процессор легко заработал на частоте 2083 МГц (против изначальной 1833 МГц), что также соответствует Athlon XP с рейтингом 2800+ (166x12.5). Причем нам не пришлось рушить или подклеивать перемычки (мостики) на корпусе процессора!



МИНЗДРАВ ПРЕДУПРЕЖДАЕТ:
КУРЕНИЕ ОПАСНО ДЛЯ ВАШЕГО ЗДОРОВЬЯ

Nikitos & Andrushock

MICROSPARC: ИС

INTRO

Так уж исторически сложилось, что в ходе технологической эволюции последних десятилетий слово "компьютер" в ушах абсолютного числа пользователей стало четко ассоциироваться с открытой шинной архитектурой персональных компьютеров. А ведь еще пару десятков лет назад внимание разработчиков было главным образом обращено на рынок "суперкомпьютеров", обладающих сверхвысокими вычислительными способностями. Это были сложные, очень дорогие системы, которые порой занимали несколько комнат, требовали огромного количества электроэнергии, совершенной системы охлаждения, а самое главное - в силу своей архитектуры почти не поддавались модернизации. Постепенно разработчики пришли к открытой шинной архитектуре, подразумевающей логическое разделение всего компьютера на суверенные совместимые между собой блоки, которые взаимодействуют друг с другом при помощи высокопроизводительных линий связи - т.н. шин.
Тут-то и начался настоящий бум: множество корпораций вступили в ожесточенную борьбу за право лидерства в этой области компьютерной индустрии, они разрабатывали принципиально различные системы, которые, однако, нашли свое применение и даже до сих пор производятся и вовсю используются. Сегодня на операционном столе компьютер германской фирмы Sun Microsystems - SPARC Station5. Интересно, что же у него внутри?



ИСТОРИЧЕСКИЕ СВЕДЕНИЯ

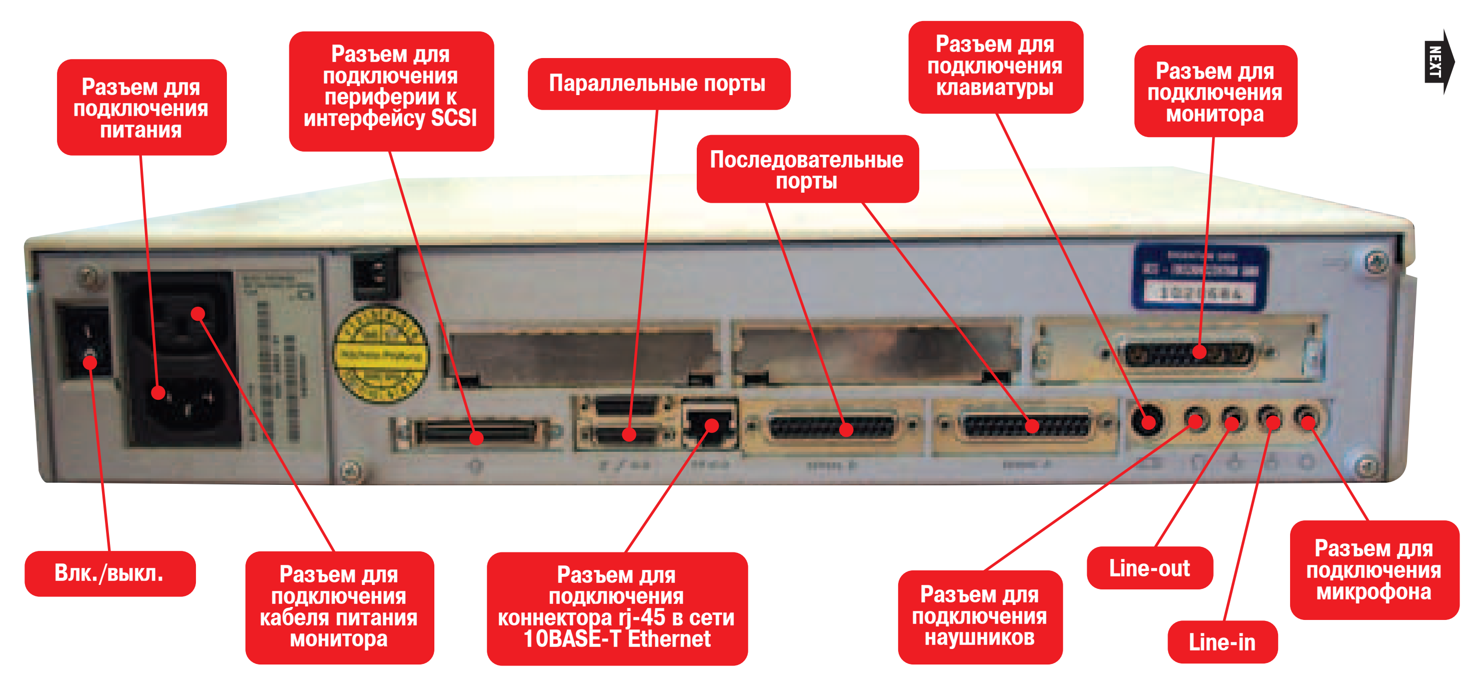
Аббревиатура SPARC расшифровывается как Scalable Processor Architecture, "Масштабируемая процессорная архитектура". Это одна из наиболее распространенных и популярных RISC-архитектур, применяемых в создании UNIX-станций и серверов. Процессоры с архитектурой SPARC лицензированы и изготавливаются по спецификациям корпорации Sun несколькими производителями, среди которых имеет смысл выделить такие конторы как Texas Instruments, Fujitsu, LSI Logic, Bipolar International Technology и Philips. Эти компании поставляют произведенные кристаллы не только самой Sun Microsystems, но и многим другим известным производителям компьютерных систем, таким как Toshiba, Matsushita, Tatting и Cray Research.
В 1990 году Sun передала все права на спарк-архитектуру организации SPARC International, которая в настоящее время включает в себя более 250 членов. Основной задачей этой организации является лицензирование технологического процесса производства кристаллов другими корпорациями, чтобы те строго придерживались спецификаций фирмы Sun. Именно четкий контроль качества выпускаемой продукции позволил процессорам PARC занять лидирующие позиции на рынке RISC-камней.
Архитектура SPARC была первой коммерческой разработкой, реализующей механизмы вытесняющей многопоточности при обработке данных. Первый процессор SPARC был изготовлен компанией Fujitsu и работал на частоте 16,67 МГц, позднее на основе этого процессора была разработана первая рабочая станция Sun-4 с производительностью 10 MIPS, представленная общественности осенью 1987 года (до этого времени компания Sun использовала в своих изделиях процессоры Motorola 680X0).
В марте 1988 года Fujitsu, под контролем Sun, увеличила тактовую частоту выпускаемых процессоров до 25 МГц, создав процессор с производительностью 15 MIPS.
Процессор SuperSPARC, чуть позже выпущенный компанией Texas Instruments, стал основой серии рабочих станций и серверов SPARCstation/SPARCserver 10 и 20.
Процессор SuperSPARC имеет внутренний кэш емкостью 36 Кб (20 Кб - кэш команд и 16 Кб - кэш данных), раздельные конвейеры целочисленной и вещественной арифметики, и при тактовой частоте 75 МГц обеспечивает производительность около 205 MIPS.
Компания Texas Instruments разработала также 50-мегагерцовый процессор MicroSPARC со встроенным кэшем емкостью 6 Кб, который ранее широко использовался в дешевых моделях рабочих станций SPARCclassic и LX. Затем Sun, совместно с Fujitsu, создала новую версию кристалла MicroSPARC II с встроенным кэшем емкостью 24 Кб. На его основе построены рабочие станции и серверы SPARCstation/SPARCserver 4 и 5, работающие на частотах до 110 МГц.
Долгое время архитектура SPARC занимала лидирующую позицию на рынке RISC-процессоров. Однако повышение тактовой частоты процессоров в 1992-1994 годах происходило невысокими темпами, и чтобы хоть как-то ускорить рост производительности, компания Sun разрабатывает и воплощает в жизнь пятилетний план модернизации существующих технологий. В соответствии с этой программой, к 1994 году Sun довела тактовую частоту процессоров MicroSPARC до 110 МГц, а годом позже выпустила новый микропроцессор SuperSpark. В ноябре 1995 года появились 64-разрядные процессоры UltraSPARC с тактовой частотой 143, 167 и 200 МГц, и UltraSPARC-II с тактовой частотой от 250 до 300 МГц, серийное производство которых началось в середине 1996 года. Позже, в 1997 году, начался выпуск процессоров UltraSPARC-III с частотой до 500 МГц.
В настоящий момент фирма Sun выпускает ряд мощных рабочих станций на базе процессоров UltraSparc-III с частотой до 1.2 GHz (стоят они порядка $7k), а также суперпроизводительные многопроцессорные серверные решения, стоимость которых может достигать десяти миллионов зеленых! Такая вот конторка.

СКРОМЕТНАЯ УСТАНОВКА!

● ПЕРВОЕ ВПЕЧАТЛЕНИЕ

Честно скажу, когда я ехал фотографировать этот компьютер, ожидал увидеть этакого мастодонта метр высотой - находился под впечатлением от осмотра старых машин фирмы Digital (PDP-16 и Dec ALPHA). Все оказалось проще, ну оно и понятно - это же рабочая станция, а не высокопроизводительный сервер. Первым делом обратил на себя внимание огромный двадцатидюймовый монитор - это чудо поддерживало 24-битный цвет, о чем сообщало при включении развеселой картинкой в углу экрана. Все элементы компьютера размещены в компактном корпусе Slim Desktop. Ну что ж, отвертку в руки, понеслась.

Первое впечатление можно сформулировать примерно так: "умеют все-таки немцы компы собирать". Немецкая тщательность и дотошность видны абсолютно повсюду, компьютер являет собой этакий конструктор Лего, каждая деталь которого плотно становится на свое место и удивительно легко, без привычных заеданий, его покидает. После снятия декоративной крышки моим глазам предстала следующая картина. Под удивительно тонким слоем пыли (этот компьютер ни разу не открывали, а выпущен он был в 1995 году), находилась материнская плата, в центре которой красовался RISC-процессор microSparc-II, никаких шлейфиков и мотка проводов не было и в помине. Удивили также 3 слота расширения для неизвестной пока шины и восемь(!) разъемов для подключения дополнительных модулей памяти DIMM.



NEXT

MICROSPARC: ИСКРОМЕТНАЯ УСТАНОВКА!



Nikitos & Andrushock



Модули установленной памяти DIMM (2x32 Mb)

Видеокарта

32-разрядный RISC-процессор устройства

Пустующие слоты для установки дополнительной памяти

Чипсет системной платы

Блок питания компьютера

Плата со SCSI разъемами

Сказевый хард от Сигейт

Слоты для подключения дополнительных устройств к шине sBus

Память видеокарты (размещена и с обратной стороны устройства)

Память видеокарты

Вспомогательный чип

Процессор видеокарты

ПРОЦЕССОР

Описываемая модель функционирует на базе RISC-процессора MicroSpark II STP1012PGA, работающего на частоте 110 MgHz. Для неосведомленного читателя следует пояснить, что на данном этапе развития компьютерных технологий существуют две основных процессорных архитектуры: CISC (Complete Instruction Set Computer, "компьютер с полным набором инструкций") и RISC (Reduced Instruction Set Computer, "компьютер с сокращенным набором инструкций"). Процессоры первой категории подразумевают наличие большого числа высокоуровневых инструкций обработки информации, машинных команд, которые иногда даже выполняются за несколько тактов. Эти процессоры характеризуются сравнительно небольшим количеством регистров и большим числом аппаратно поддерживаемых команд (в некоторых процессорах даже присутствуют инструкции работы с mp3-звуком, кодеком div'x и т.д.). Понятно, что любая, даже самая сложная операция, может быть представлена в виде композиции конечного числа элементарных дискретных шагов. Обработку информации в этом случае можно представить себе в виде конвейера на заводе - над информацией поочередно выполняются какие-то элементарные операции, которые придают ей необходимую форму.

Как выяснилось, такой путь эффективнее в ряде случаев, но далеко не всегда. Есть класс задач, в которых такой подход показывает себя с худшей стороны. На самом деле, правда, как всегда, посередине - при использовании как CISC, так и RISC-архитектур в чистом виде, появляются совершенно абсурдные моменты. Так, например, особо фанатичные RISC-производители, отказываясь от аппаратно реализованного оператора умножения чисел, предлагают системным программистам заменять его многократным сложением (к слову, аппаратная реализация оператора умножения работает так же). Однако вставал вопрос: как же быть, если религия RISC не позволяет им ввести на аппаратный уровень оператор цикла? :)

По этой причине в современных системах используется гибрид этих технологий, в чистом виде они уже почти не применяются.

В девяностых годах инженерный коллектив компании Sun столкнулся с проблемой невозможности дальнейшего повышения производительности выпускаемых систем посредством наращивания частот процессоров, оставляя их конкурентоспособными на рынке рабочих станций. Выход был один - повышать эффективность представления и обработки информации в уже существующих процессорах, модифицируя наиболее рациональным образом набор команд и выстраивая многопотоковую конвейерную систему.

Разработанное решение было воплощено в процессоре MicroSparc II. Этот кристалл представляет собой высокоинтегрированную микросхему, состоящую из арифметико-логического устройства (которое включает в себя блоки целочисленной и вещественной арифметики), устройства управления регистрами, а также множества разделенных регистров команд и данных.

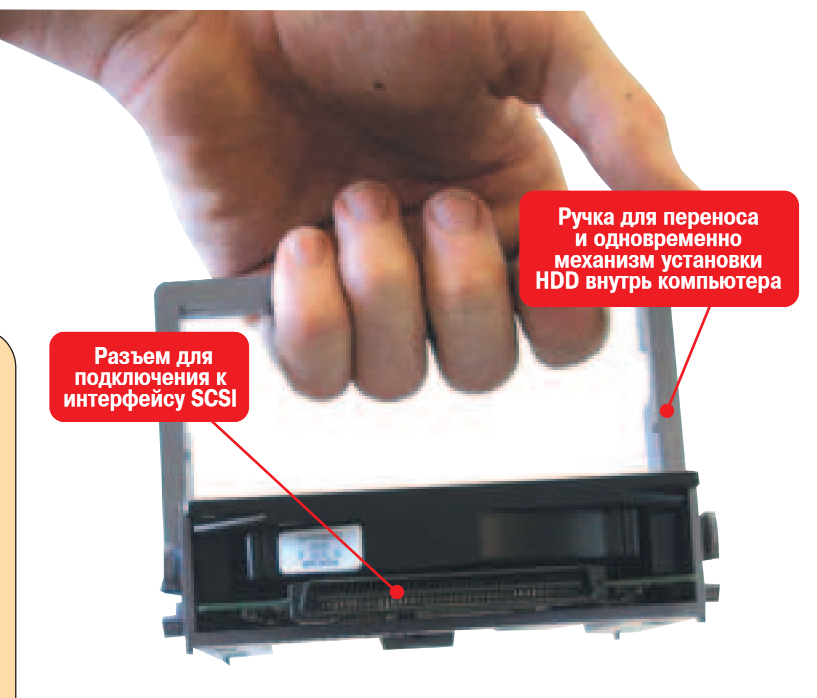
Блок целочисленной арифметики в этом процессоре представляет собой практически совершенную систему: пятиступенчатый высокопроизводительный конвейер, эффективно взаимодействующий с регистрами и способный одновременно выполнять до двух команд.

Процессор microSPARC II имеет также 64-разрядную шину данных для связи с памятью и может адресоваться к оперативной памяти объемом до 256 Мб. В процессоре также интегрирован контроллер шины SBus, обеспечивающий эффективную, с точки зрения стоимости, реализацию процедур ввода/вывода информации.

MICROSPARC: ИСКРОМЕТНАЯ УСТАНОВКА!



Nikitos & Andrushock

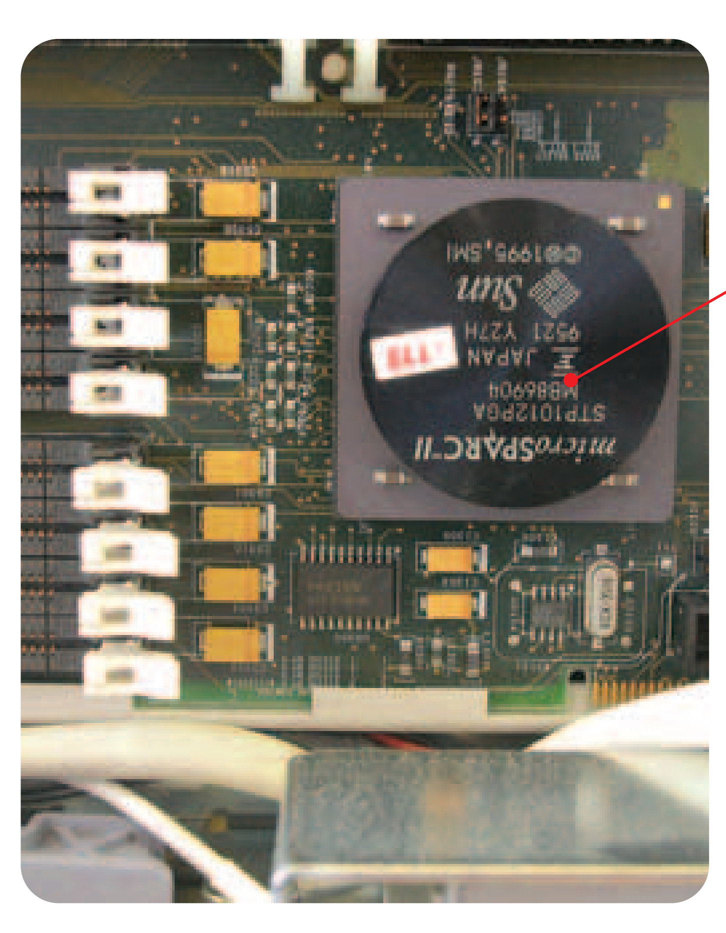


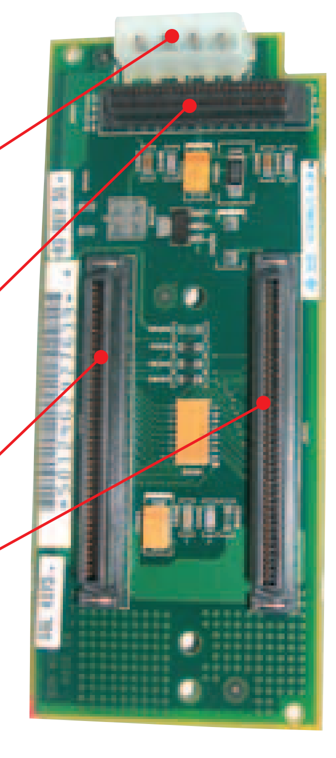
СИСТЕМНАЯ ПЛАТА

Системная плата Sparc Station5 представляет собой обыкновенную печатную плату, на которой расположены управляющие компьютером элементы, и по внешнему виду мало чем отличается от обыкновенной PC'шной материнки. Однако если рассмотреть ее поближе, появляется масса интересных моментов и всплывает множество не затрагиваемых ранее тем. Во-первых, в этом компьютере не используются такие популярные шины, как PCI и AGP - для подключения дополнительных устройств применяется 32-разрядная шина sBus, обеспечивающая полосу пропускания до 200 мегабайт в секунду и работающая на частоте до 25 мегагерц.
К этой шине может подключаться как видеоадаптер, так и любые другие дополнительные устройства (сетевые и аудио карты, модемы, контроллеры, etc).
Разработанная в 1989 г. исключительно для внутреннего использования, эта шина была подхвачена остальными производителями, в результате чего полторы сотни фирм так или иначе стали использовать ее в своих изделиях. Такая популярность шины была объяснима тем, что она чуть ли не единственная на тот момент умела автоматически транслировать виртуальные адреса в физические, распознавать ошибки при передаче данных и инициировать повторы, в результате чего работала очень шустро для тех времен.
Описываемая материнская плата имеет множество интегрированных в чипсет устройств - это 10BASE-T Ethernet контроллер, звуковая карта, а также параллельные и последовательные порты.
Для взаимодействия с накопителями данных (HDD, CD-ROM) применяется интерфейс SCSI (принято читать как "скази"), обеспечивающий высокую скорость передачи данных в режиме DMA (Direct Memory Access). К материнской плате отдельным модулем подключается панелька, на которой расположены разъемы для подключения скази-устройств.
В качестве оперативной памяти используется специфичная для SPARC-архитектуры память стандарта DIMM со временем доступа около 60 наносекунд.

ДОПОЛНИТЕЛЬНЫЕ ФИШКИ

Особо порадовала комплектация этого компьютера. В поставку включалась полная лицензионная версия коммерческой Unix-like ОС Sun Solaris (в народе "солярка"), под управлением которой компьютер обещал работать еще быстрее (к слову, на ряде тестов он показывал производительность на уровне P-166 mghz).
Интегрированные на материнской плате средства позволяют использовать этот Спарк в качестве сетевой рабочей станции, не приобретая дополнительных устройств. Также в материнскую плату интегрирована звуковая карта, к которой подключен маленький динамик, способный издавать на удивление мелодичные звуки, в отдельные моменты напоминая телефон с полифонией :). Порадовал и прилагающийся к монитору маленький пультик, с помощью которого можно издали менять его настройки.
Самая же модная фича заключается в том, что жесткий диск подключается к SCII-плате без всяких там шлейфиков, при помощи хитрого механизма. HDD помещается в специальный короб, оборудованный ручкой для переноса. Это короб помещается внутрь корпуса компьютера и, при опускании ручки, жесткий диск механическим путем поджимается к скази-плате, подключаясь к интерфейсу передачи данных и разъемам питания. Весь процесс извлечения и установки жесткого диска можно выполнить менее чем за секунду, что лично меня привело в неописуемый восторг :).








С вами мы –
Суппер-Группер!
Я – МС Рупор
Начни сбор –
полный набор!
Собери весь
«Super-Группер».
Будет экстаз!
Ах класс!
Sprite®
АРТ-ЖАЖДА
представляет
«Super-Группер»
The Coca-Cola Company против уличного вандализма и хулиганства. Sprite является зарегистрированным товарным знаком The Coca-Cola Company. ©2003 The Coca-Cola Company. Напиток сертифицирован.

Ст. о/у Goblin



– ДЕЙСТВОВАТЬ СМЕЛО. НИКОГО НЕ РАССПРАШИВАТЬ. ПОБОЛЬШЕ ЦИНИЗМА. ЛЮДЯМ ЭТО НРАВИТСЯ.

О. БЕНДЕР, «ДВЕНАДЦАТЬ СТУЛЬЕВ»

Сделано с особым цинизмом



<Былое и думы>

Давным-давно, аж в начале прошлого века, дедушка Ленин сказал: из всех искусств для нас важнейшим является кино! И хотя вождь мирового пролетариата со всеми своими идеями пролетел, как трусы над баней, в данном вопросе он оказался прав.
Только самого важного Ильич не прос к: самым важным оказалось кино не большевистское, а буржуинское. Как-то так получилось, что западное кино и поярче, и покрасочнее, да и в целом получше. Причем значительно.
Когда рухнул Железный Занавес, фильмы поперли в страну Советов мощным потоком. Фильмы были все больше американские. А граждане самой грамотной и самой читающей на свете страны иностранных языков отчего-то не знали. Но земля русская богата талантами. И за дело взялись специально обученные люди.
Дом, в котором имелся в наличии видик, считался домом состоятельным. Видик - вот что оказалось главным связующим звеном с Цивилизацией. В доме счастливого владельца постоянно норовили собраться на вожделенный просмотр граждане классом пониже. Видик заглатывал потасканную кассету. Аудитория замирала, и начинался фильм. Отвратного качества изображение сопровождал не менее отвратный звук. А поверх всего этого звучал заикающийся гнусавый голос неизвестного переводчика.
На экране яростно визжал Брюс Ли, строил зверские рожи Сталлоне, железной поступью шагал по трупам Арнольд. Разинув рты, народ приобщался к Великому.
Но по мере отхода от первых восторгов, стало заметно, что гнусавый переводчик и его товарищи по цеху обращались с материалом несколько вольно.
То, что получалось в итоге, в большинстве случаев назвать переводом можно было только с большой натяжкой. Переводили они поточно-конвейерным методом, пару-тройку фильмов в день. Переводили "на слух" и с первого просмотра, что трагическим образом сказывалось на качестве. Непонятные и сложные места - без затей пропускались, богатые монологи - сокращалось, непонятные шутки - заменялись самодельными. Получившееся в итоге переводом назвать было сложно. Это был не перевод, а вольный пересказ. Пересказ того, что переводчик смог разобрать на слух а потом успел сказать в микрофон.
Выбора в те времена не было. Как говорится, "За неимением хозяйки - сгодится и кухарка". В обществе тотального дефицита - хавай, что дают. И народ хавал. Хотя многих тошнило.
Если хочешь, чтобы было как следует - делай сам!

В начале девяностых, в те дикие времена беспредельного бандитизма и тотальной криминализации общества у моего приятеля Вована был мегавидик, который позволял накладывать звук - большая по тем временам редкость. А еще у него была одна из самых больших в Питере коллекций фильмов. Причем - в оригинале, полный шкаф шедевров мирового кинематографа на самых настоящих западных видеокассетах.
Мы регулярно подвергали их просмотру, плевались от убогих переводов и вынашивали коварные планы перево-дить все это дело самостоятельно. Переводить так, чтобы приятно было смотреть самим и не стыдно показывать другим. А это значит - максимально адекватно и без купюр. Как следует, по-взрослому.
Тут следует пояснить тем, кто вдруг не знает. Американские фильмы в большинстве своем изобилуют нецензурной бранью. В данном вопросе, как и во многих других, они нас обскакали лет на пятьдесят. Это я не к тому, что "ай, как здорово - они в фильмах ругаются!". А к тому, что творец - режиссер и сценарист, может строить свое произведение так, как ему хочется. Возрастной ценз на просмотр подобных фильмов - безусловно, есть. Но вот цензуры в нашем понимании - там нет. Мы до такого пока что не доросли. Нам и цензоров не надо, у нас переводчики есть - они сами все зацензурят по собственному разумению.
Ну, и как-то раз чаша терпения переполнилась: я напялил наушники, вооружился авторучкой и решительно взялся за блокбастер "Путь Карлито". Сколько времени отнял первый демарш - точно уже не помню. Помню, что много. Изведя пару авторучек и густо покрыв яростными каракулями тридцать листов бумаги, Карлито я заборол.
Готовый фильм отличался от привычного радикально: наконец-то прояснились все непонятные мести, а бандюки заговорили так, как подобает бандюкам! Мы с Вованом были в полном восторге. Однако восторг разделяли не все. Наше сообщество раскололось пополам: одна половина содеянное одобряла, другая - решительно отвергала. На вопрос "А что не так?" следовал решительный ответ: уберите из фильма нецензурную брань! В ответ на что я отвечал: не я ее туда вставлял, не мне ее оттуда и убирать.
Спорили долго и нудно. Спорим до сих пор. Никакого согласия достичь тогда не удалось, не удается достичь его и теперь. А я про себя решил: делать надо так, как считаешь правильным ты сам, а не угождать вкусам посторонних.
После этого перевел в том же духе еще несколько фильмов. Однако техническая сторона процесса была настолько непростой и требовала настолько больших затрат времени, что увлечение очень быстро закончилось.

<Здесь и сейчас>

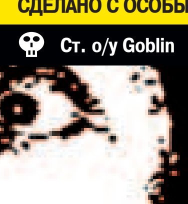
Прошло семь лет. Появились компьютеры. А в компьютерах появились проигрыватели DVD. И я купил себе первый фильм - Desperado Родригеса. Восторгам не было предела: отличное качество изображения, прекрасный звук, полное отсутствие идиотских переводов плюс наличие английских субтитров! Немедленно зачесались руки, и я взялся за работу.
Как известно, при наличии некоторых навыков, возня на компьютере с любым видом информации - занятие довольно несложное. Перво-наперво я набрал текст перевода. Потом распечатал его и отредактировал. Затем раздобыл поганенький микрофон, воткнул его в звуковую карту. После этого наживил полезную софтину под названием Sound Forge и по ходу фильма зачитал текст. По окончании кое-что подправил, и - бэмс! Получился отличный, готовый к употреблению перевод!
Как водится, фильм заиграл совершенно новыми

NEXT

PC_Zone

СДЕЛАНО С ОСОБЫМ ЦИНИЗМОМ

Ст. о/у Goblin

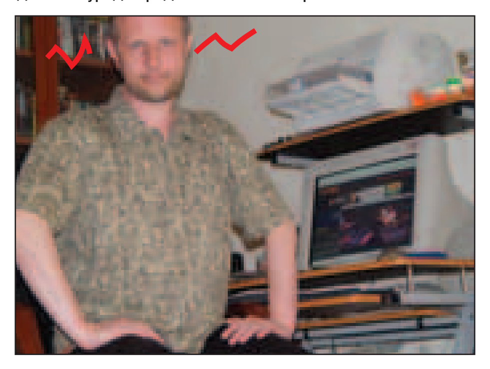






красками. Друзья и товарищи снова были в восторге. И закипела работа.

Следующим кандидатом был фильм "От заката до рассвета". В том варианте, что показывают по телевизору, братья Сет и Ричи Гекко, которых играют Клуни и Тарантино - два этаких разудалых весельчака. На самом же деле это два отморозка, всю первую часть фильма ничего, кроме омерзения, не вызывающих. Во второй же половине фильма они попадают в такой жуткий переплет, что даже две такие мрази поневоле начинают вызывать сочувствие. Именно в этом, по словам режиссера Робрта Родригеса, и заключается сценарный замысел. Ну, в моем переводе два этих урода предстали в полной красе.



Было принято решение организовать собственную студию. Студия была названа "полный Пэ" - думаю, не надо объяснять, почему. А дальше поперло: "Криминальное чтиво", где Винсент и Джулз наконец-то заговорили, как подобает настоящим тупым подонкам, "Цельнометаллическая оболочка", где я припомнил собственную бытность сержантом Красной Армии, и, наконец, "Большой куш", в котором особо ярко проявились познания, приобретенные на службе в уголовном розыске.

"Большой куш" (он же Snatch, что в моем переводе звучит непечатно) произвел фурор. К нему, в отличие от "Карты, деньги, два ствола", общественность еще не успела привыкнуть. Никто не сравнивал его с другими, люди просто смотрели фильм. Перевод появился в нужное время в нужном месте и оказался просто бомбой.

Следует отметить главное: фильм сам по себе - очень хороший и очень смешной. Перевод - дело сугубо вторичное. Однако то, что тамошние бандюки заговорили на нормальном русском языке, народу страшно понравилось. Ну и понеслось.

Со временем я обзавелся добротным оборудованием: теперь у меня качественный микрофон Rode, знатная карточка для записи звука Audiofile. Из софта пользую все тот же Sound Forge. Непрерывные апгрейды уверенно ведут к тому, что работать становится все легче. И это не может не радовать, потому что растет и качество, и производительность.

<Акция и реакция>

Несмотря на одобрение большинства, имеется и масса недовольных. Одно время жаркие словесные баталии велись на моем сайте www.oper.ru непрерывно. Тех, кто рассказывает о том, что "в английском языке мата нет", я изначально игнорирую как безграмотных идиотов. На все претензии отвечаю одинаково: не нравится, как делаю я - сделай так, как нравится тебе. И все будут довольны.

Но больше претензий другого рода. В ходе продолжительных филологических дискуссий по поводу различных аспектов перевода мне неоднократно сообщали, что если фильм откровенно тупой, но переводчик удачно пошутил (читай - спорол отсебятину), значит, шутки переводчика идут строго на пользу фильму.

На мои осторожные предположения о том, что таким образом нагло искажается сущность авторского замысла, мне отвечали: мол, нет в тебе божьей искры, и потому тебе, серому ремесленнику, подобных тонкостей не понять. Вот раньше были люди...

Через это под волосатым крылом легендарной студии "полный Пэ" мной был создан мегапроект "Божья искра". В рамках проекта планировалось создавать "переводы", авторов которых ни грамма не интересует то, что хотели сказать/показать сценарист и режиссер. Личный состав проекта "Божья искра" может и умеет ярко шутить! У меня не было никаких сомнений в том, что переведенные новым, безусловно прогрессивным методом, фильмы окажутся настоящим открытием для зрителей.

Для начала выбрали жертву - над чем будем глумиться. Поскольку я терпеть не могу сериал "Звездные войны", то под раздачу назначили его. Но пока искали нужные DVD, решили сделать "Властелина колец", к которому я, напротив, отношусь положительно. Сценарий был слегка переколбашен: всех положительных героев обозначили как милиционеров и вообще правильных парней, а всех отрицательных - как уголовников и вообще фашистов. Попутно переколбасили все имена, и в фильме появились хоббит Федор Сумкин, его друг Сеня Ганджубас, майор-волшебник Пендальф, царь Агроном, прибалтийский эльф Логоваз, гном Гиви и оперуполномоченный ГУВД Гондураса Баралгин. Естественно, все они постоянно несли разную чушь, не имеющую никакого отношения к происходящему на экране. Кроме того, наглым образом снабдили звуковую дорожку всякой музыкой: злым силам навтыкали Рамштайна, а добрым - всякой отечественной попсы.

Эффект выпуска первого продукта "Божьей искры" превзошел все ожидания. Никто, в общем-то, и не понял, что это откровенный стеб над плохими переводчиками и тупыми зрителями. Нудноватый, в общем-то, фильм внезапно заиграл свежими, невиданными доселе красками, и зажил своей собственной жизнью.

Шуток мы там нашутили так богато (шутили толпой: главным был мой камрад Сидор Лютый, вместе с ним - я, и еще целая толпа народа с моего форума), что потом весь фильм растащили на цитаты.

Что характерно, для "Властелина" я сделал и нормальный перевод. Однако "Божья искра" зарулила все: на триста отзывов о глумливом "переводе" приходится ровно один про перевод нормальный.

Ну, мы не растерялись и тут же забомбили продолжение, которое называется "Две сорванные башни". Во второй серии бывший мордовский интеллигент Голый ведет на свою малую родину носителя зловредного кольца Федора Сумкина и его друга Сеню Ганджубаса. Агроном, Гиви и Логоваз ведут преследование банды педофилов из первой серии. Сарумян, сын Вассермана и шестерка Саурона, осуществляет акт агрессии против Незалежной Рохляндии. Перед лицом нависшей опасности сильно пьющий атаман Борис принимает решение всем колхозом спрятаться на даче. На помощь обороняющимся дачникам подтягиваются Саша Белый со своей бригадой и заградотряд эльфийских стрелков "Белые колготки". Считаю, что накал тупизны остался прежним, "перевод" получился ничуть не менее идиотским, чем первый.

В настоящее время "Божья искра" заканчивает работу над первым эпизодом "Звездных войн", на очереди - эпизоды четвертый и шестой. Ну и, само собой, под раздачу уже попала первая серия "Матрицы".

<Вопросы и ответы>

Народ постоянно задает вопросы: что требуется для того, чтобы ловко переводить фильмы? Себя я большим специалистом не считаю - так, старательный любитель. Однако отвечаю: ничего хитрого не требуется.

Перво-наперво, надо свободно владеть своим собственным языком. Ибо переводить будешь на русский, и фраз типа "Это очень сильное колдунство!" в переводе на русский быть не должно.

Во-вторых, надо хорошо знать английский. А это значит - несколько лет упорного труда. Язык невозможно выучить по книжкам "Английский для идиотов - за десять занятий!". Можно учить особо прогрессивными методами, но все равно и это - годы упорных занятий. Я тут и сам подумываю, не пойти ли на курсы английского.

Ну и, в-третьих, следует иметь хорошую эрудицию: разбираться в Библии, греческой мифологии, знать имена богов, названия планет, разбираться в географии, археологии, истории, машинах, кораблях, вертолетах, оружии, знать медицинскую, армейскую, полицейскую и юридическую терминологию, понимать наркоманский и негритянский жаргоны и еще очень много чего надо знать.

Без эрудиции - никуда, потому что фильмы снимают про все на свете, а переводить - тебе одному.

<Планы>

В настоящее время домашняя забава приобретает серьезный размах. По городу на всех лотках лежат диски и кассеты с надписью "Перевод Goblina". Что не может не радовать. Сейчас планирую забабахать переводы всех фильмов Тарантино и Скорсези, плотно заняться фильмами военной тематики и от души поработать над любимыми мультфильмами.

Так что - забегайте на www.oper.ru, следите за новостями.



Тарифные планы для тех, кому нужна качественная связь в сочетании с разумными затратами

Оптима День
- Тариф для тех, кто делает большинство звонков в дневное время.
- 2 «Любимых номера» включены в абонентскую плату.
- Низкая стоимость исходящих звонков внутри сети.

Оптима Вечер
- Тариф для тех, кто преимущественно общается в вечернее время.
- Скидка 50% на звонки с 20.00 до 8.00 ежедневно.
- 1 «Любимый номер» включен в абонентскую плату.

Оптима Универсал
- Тариф для тех, кто делает большинство звонков на городские телефоны.
- Городские звонки по цене внутрисетевых.
- Скидка 50% на звонки с 20.00 до 8.00 ежедневно.

Оптима Плюс
- Тарифы без абонентской платы с предоплаченными минутами.

МТС. ОПТИМА
соответствовать уровню

Основные преимущества:
- Скидка 50% на местные и внутрисетевые звонки с 20.00 до 08.00.
- Детализированный отчет по балансу — 0 у.е.
- Входящие вызовы с телефонов МТС — 0 у.е.
- Низкая стоимость звонков на «Любимые номера».
- Возможность подключить 3 «Любимых номера».
- Скидка 50% на местные и внутрисетевые звонки в выходные дни круглосуточно (при наличии услуги «Выходной день»).
- Звонки в область по цене городских звонков по дневному тарифу.



Все цены приведены без учета НДС и НсП.

Лицензия Министерства РФ по связи и информатизации №14665. Товар сертифицирован.

A.P.$lasH (ap-slash@tfs.kiev.ua)



CD ПОД ЗАЩИТОЙ

Однажды в тесном кругу моих веселых соплеменников проходил спонтанный джем-сейшн. Результаты фиксировались на обSHARPанный кассетник "для наших детей и прочих поклонников". Когда прогремел финальный аккорд очередной нетленки, мы отложили в сторону медиаторы и не спеша принялись обсуждать лицензионные достоинства нашей общей знакомой. Интересно, почему никто не догадался выключить запись? В тот же вечер кассета оказалась у нее в руках. Когда я наконец сообразил, какая угроза нависла над моим утонченным имиджем, время было уже недетское.

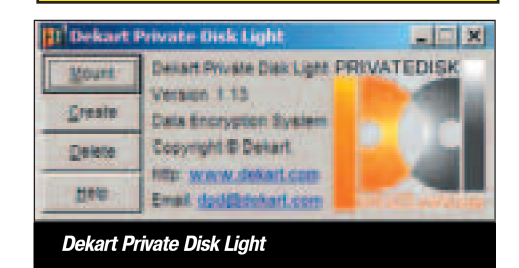
КАК СПРЯТАТЬ ИНФОРМАЦИЮ НА КОМПАКТЕ

<Теория>

Что ни говори, конфиденциальная информация существовала во все времена, но если раньше ее хранили в отдельных папках с грифом "Ноги оторву", то сейчас кругом одни винчестеры. На них весь компромат свален в кучу - и поквартальный отчет, и ненаглядная диссертация, и "Тетя Франя с Пашей в бане". Информация поджимает хвост и требует защиты. Призадумаемся... Что проще украсть - слиток золота или вагон червонцев, разбросанных по всей квартире? Вот именно. Предлагаю все жизненно важные файлы тщательно зашифровать и перебросить на энное количество компактов.

ACE/RAR/ZIP с паролем - вещь хорошая, но требует распаковки на диск. Собираешься активно работать с несколькими архивами? Приготовься многократно вводить пароль. Не подходит, отбрасываем. Лично мне приглянулась идея создавать так называемые зашифрованные контейнеры. Что это такое? Ничем не примечательные файлы на винчестере, которые по желанию можно подключить в системе как отдельные диски. Казалось бы, работаешь с настоящим винчом, однако данные при этом хранятся в зашифрованном виде - triple DES, Blowfish... Волшебные слова. Если переместить контейнер на CDR, то изменить его содержимое ты уже не сможешь, но зато без проблем спрячешь диск в нагрудный карман пиджака, поработаешь с ним за машиной приятеля и раздраконишь об колено в случае опасности. Осталось подобрать подходящий софт.

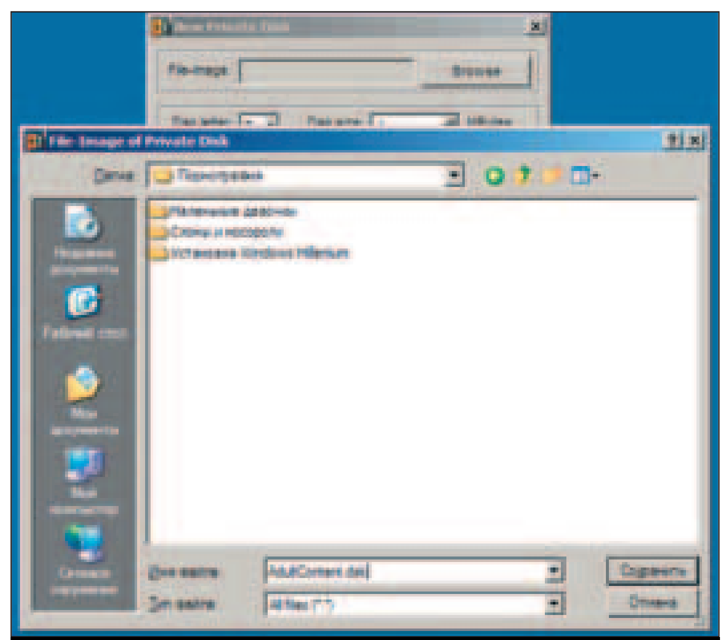
<Dekart Private Disk>



Dekart Private Disk Light

Один из самых скромных вариантов, однако это не умаляет его достоинств. Запускай. На экране миниатюрное окошко с логотипом и контактными данными,

причем это даже не сплэш-скрин, это и есть твой пульт управления. Декартовцы стараются быть проще и ждут, когда к ним потянутся люди. Мне кажется, народ мимо не проходит. Всего четыре кнопки - "Mount" (Подключить диск), "Create" (Создать новый), "Delete" (Изничтожить в клочья) и "Help" (Справочная). Нажимай на "Create" и понеслась… В появившемся диалоговом окне PDL (назову его так для краткости, OK?) предлагает выбрать файл, в который программа запишет содержимое будущего диска. Поле называется File-image. Рядом есть кнопка "Browse" (Обзор). Нажми на нее и расскажи программе, где ты собираешься хранить свои маленькие тайны. В том же самом окне можно указать размер и букву для будущего носителя информации. Разобрался? Отлично. И снова мы падаем на кнопку "Create". PDL предлагает ввести пароль на доступ к своему детищу (не менее пяти символов) и рисует красивый индикатор работы. Из динамиков раздается вкрадчивое "Форматни меня, папа!" Это твой новый диск. И не вздумай отказаться.



Dekart Private Disk Light - Новый диск

FAT, FAT32, NTFS… Не имеет значения, что ты выберешь. Важно лишь то, что после форматирования диск будет автоматически установлен в системе, и пока он находится во власти PDL, доступ к файлу для остальных приложений заблокирован. Ни прочитать, ни забить нулями. Кроме того, кнопка "Подключить новый диск" сменила фамилию. Теперь это "Dismount". Нажми на нее, когда закончишь работать с диском, и открой файл на чтение. Что, простите? Нет, это не XOR, это AES (Advanced Encryption Standard), которым Dekart шифрует данные своего пользователя. Дело за малым - скинуть на новый диск свои страшные секреты и переписать файл на CD. Дальше - проще. Отдаем компакт на съедение CD-вертушке и запускаем PDL следующим образом - PrvDiskLight.exe /path:Путь_к_файлу_с_диском /password:Твой_оригинальный_пароль. При желании можно создать ярлык на рабочем столе, но тогда последний ключ лучше пропустить, верно?

Dekart Private Disk Light

Описание от разработчиков
http://www.dekart.com/?id=2304

Ссылка на закачку
http://www.dekart.com/pub/PrvDiskLight.exe

Его старший брат - Dekart Private Disk

Описание от разработчиков
http://www.dekart.com/?id=2125

Напоследок - о недостатках. Одна копия PDL может разродиться только одним диском - на то она и Light. В принципе, если стартовать программу с параметром /multi, то запустится новый экземпляр PDL, и ты сможешь подключить еще одну коллекцию секретов, но при этом в трее появится очередная иконка программы. Я считаю, что вереница красных и зеленых шариков (именно так выглядит иконка) хорошо смотрится только на новогодней елке. Кроме того, специальная комбинация клавиш Ctrl+F12, которая позволяет отключить текущий диск, действует на все копии PDL одновременно. А что ты скажешь по поводу размера? Его можно указать только при создании нового контейнера, и если тебя со временем перестанет устраивать начальная емкость, то вариант один - удаляем старый носитель и начинаем все с самого начала. В остальном - достойный вариант для неприхотливого пользователя.

<Best Crypt>

Обожаю программы, которые после установки требуют перезагрузить машину. Правильно, пусть пользователь рыдает и кланяется при каждом запуске этого монстра - серьезные люди старались, неделю кофе пили. В данном случае Best Crypt собирает-

PC_Zone

CD ПОД ЗАЩИТОЙ

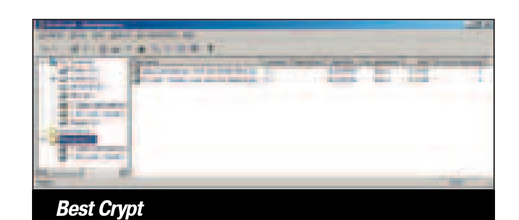
A.P.$lasH (ap-slash@tfs.kiev.ua)

TIPS&TRICKS

Меня, как и многих других, раздражает то, что некоторые сайты насильно делают свои страницы стартовыми, а иногда это еще сложно исправляется, так как они любят делать записи в реестре. Ну, так вот, чтоб не быть самым лысым, делаем следующее: в свойствах ярлыка Эксплорера, в поле "объект" дописываем флаг -nohome (у меня, например, так: "C:\Program Files\Internet Explorer\IEXPLORE.EXE" -nohome). Приятных рейдов по порно сайтам ;).

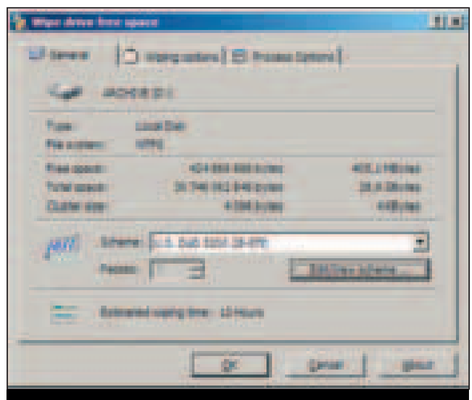
Matvey
xa110now@yandex.ru

Хочешь увидеть свои советы в журнале? Присылай их на адрес Sklyarov@real.xakep.ru. Ведущий рубрики Tips&Tricks Иван Скляров.



Best Crypt

ся активизировать защиту твоих будущих дисков. Отныне JBC файлы удалить нельзя, так как они по умолчанию считаются контейнерами программы. Спору нет, возможностей у данного приложения намного больше, чем у PDL. Начнем со списка поддерживаемых алгоритмов. Best Crypt предлагает уже знакомый нам AES, а также TwoFish, BlowFish и GOST - Government Standard of the USSR (наши в городе!). Ты сможешь не только подключать неограниченное количество дисков, но и объединять их в группы (компромат, фотографии падших женщин, оригинальные рецепты абсента), причем благодаря параметру AutoMount подключение будет происходить автоматом при старте системы - только успевай вводить пароли.



Best Crypt - Вычищаем опустевшие кластеры

Товарищи, паранойя осложнений не дает, болеют все! Резидентная защита контейнеров от удаления - не предел. Best Crypt умеет вычищать свободное место на диске и безвозвратно уничтожать любые файлы (в комплекте поставляется дополнительная утилита BCWipe), прячет свою иконку в системном трее и (барабанная дробь) шифрует файл подкачки. Бедная винда... Единственное, чем я так и не смог проникнуться, это Timeout - при отсутствии активности со стороны пользователя отключаются все установленные диски. Интервал срабатывания - на твое усмотрение. Вот только кто мне объяснит, зачем это нужно? Допустим, ты эмигрировал в Нью-Йорк и живешь в Бронксе. Утром идешь на работу, квартиру оставляешь открытой и говоришь дочке: "Машенька, наш супер-пупер стальной замок на таймауте. Если на пороге появится злой негр, заболтай дядю на пару минут и дверь прищемит ему башку". Есть же специальная комбинация клавиш для отключения дисков. Или это для тех, кому за 70, на случай спонтанного атеросклероза?

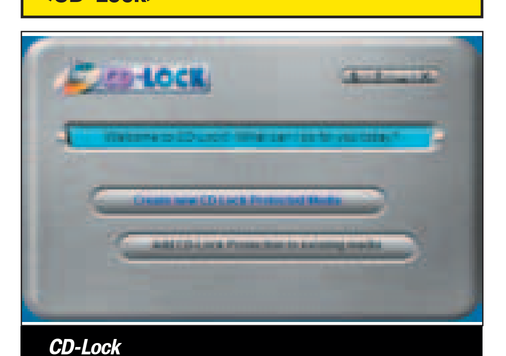
Процесс создания нового диска мало чем отличается от предыдущей утилиты. Выбираем в главном меню панели управления пункт "Container - New container", указываем файл для записи образа и алгоритм шифрования. После ввода пароля (на сей раз - не меньше восьми знаков) программа отформатирует диск и установит его в системе. Как и прежде, никто не помешает нам закатать свежесозданный контейнер на болванку и положить рядом с ним установочный архив BestCrypt. Осталось трижды восхититься продуманным и весьма симпатичным интерфейсом программы, а также отметить заманчивую возможность комплектовать ее собственными плагинами. Development Kit лежит на сайте у разработчиков. Справочный файл доверительно сообщает, что теоретически возможно прикрутить к программе распознавание отпечатков пальцев ее владельца. Никаких паролей - приложил палец к... (не уточняется) и порядок. То ли еще будет...

Best Crypt
http://www.jetico.com

BestCrypt Development Kit
http://www.jetico.com/bdk.exe

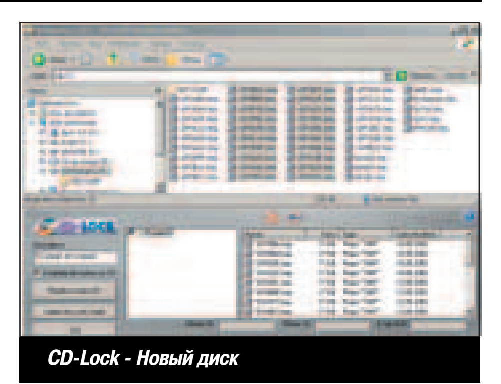
BestCrypt for DOS/Windows 3.1 (freeware)
http://www.jetico.com/bc_free.exe

<CD-Lock>



CD-Lock

Экспонат номер следующий решительно выбивается из общего строя. CD-Lock не умеет создавать отдельные контейнеры, но со счетов эту приблуду так просто не сбросишь. Разработчики заверяют общественность в том, что их детище в состоянии защитить любой съемный диск. Посмотрим, как у него обстоят дела с компактами. На первый взгляд - простенькая нарядная игрушка (причем дорогая - 20 зеленых), а как сядешь почитать документацию... "Тут вы играете, тут вы не играете, тут мы рыбу заворачивали". Основная мысль заключается в том, что CD-Lock без проблем зашифрует файлы при помощи BlowFish, а также опционально исковеркает их имена. В том же каталоге программа создает autorun.inf, который запускает дешифратор. Если в системе установлен движок от Roxio, то CD-Lock самостоятельно закатает на болванку весь комплект, включая дешифратор и его вспомогательные файлы. Запускаем программу. CD-Lock предлагает на выбор два возможных действия - "Create new CD-Lock protected media" для создания нового диска и "Add CD-Lock protection for existing media" для защиты уже существующего. Попроси выполнить первое действие и приготовь болванку. Программа поинтересуется, какой у нас тип носителя. Выбирай "Read-only" и не забудь сказать, что у тебя мало времени. Как это сделать? Ну, я даже не знаю... Ногой топни. Следующий вопрос в том, нужно ли сохранять во временной папке твои файлы. Другими словами, будешь ли ты записывать их на другой компакт в ближайшее время? Не думаю. Откажись. Пароль на доступ к диску можно ввести любого размера - программа покладистая и в советчики не набивается. Писать вместо настоящих имен файлов абракадабру (Scramble file names) или нет - решай сам. В итоге на рабочем столе появляется стандартный Проводник, венчающий окошко CD-Lock. Перетаскиваешь файлы из проводника на панель программы, фиксируя боковым зрением кнопку "Ready to make CD" (Готово, вашсокбродь!).



CD-Lock - Новый диск

CDLock
http://www.cd-lock.com

Ссылка на закачку
http://www.cd-lock.com/cdl.exe

Диском я остался доволен. Дешифратор стоит в автозагрузке. Ввел пароль - работаешь с файлами в свое удовольствие. Отказался (не знаешь/забыл) - читаешь абракадабру, постигаешь вечность. От самой программы ощущения остались двойственные. Не совсем понятно, зачем ей скины. Это ведь не плеер. Взяли бердданку и обшили бисером. Кроме того, это даже не скин. Это фотография оцинкованного ведра. Зашли к уборщице, взяли на пару дней (ведро, конечно же, не уборщицу). Идея таскать за собой Проводник и растягивать его под свои размеры - отдельный разговор. Тем не менее, диск получился очень хороший. Ничего устанавливать не нужно, все стартует автоматически. Одно плохо - разработчики утверждают, что на версиях Windows младше 2000/XP дешифрованные файлы временно сохраняются на диск. Соответственно, в дальнейшем их можно восстановить. Не забывай об этом.

<Strong Disk Pro>

Луч света в темном царстве. Наконец-то НАША программа. Родная, русскоязычная. Она вполне может оказаться лучшей из всех, рассмотренных ранее. Сейчас проверим. Сразу же после первого запуска тебя аккуратно берет в оборот специальный мастер по созданию и подключению нового контейнера. На каждом этапе установки Strong Disk снабжает хозяина подробными комментариями от разработчиков, причем львиной долей драгоценной информации с тобой поделится справочный файл. Таблица производительности алгоритмов шифрования, рекомендации по выбору паролей, совместимость с другими приложениями. А ведь во многих русскоязычных программах справка до того страшная и безграмотная, что во время ее прочтения постоянно хочется выпить. И ни в коем случае не закусывать.

PC_Zone

TIPS&TRICKS

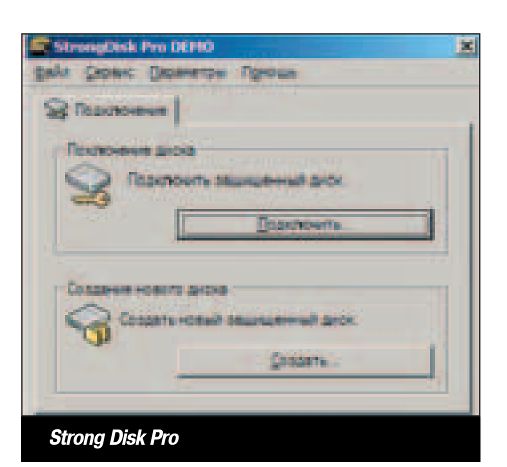
Прокатывает на олимпиадах по ИВТ. Бывает, что участников сажают за компьютеры для проверки и отлаживания кода. Сейчас в большинстве кабинетов компы подрублены к сети. В QBasic можно сделать свой собственный shell и, используя команды, прошарить сетку на предмет уже решенных заданий той же олимпиады :). После использования shell "net use * \\ip\path" и т.д. у меня, благодаря такой наглости, из воздуха появилось 3 задания из четырех, и все они оказались правильными. В общем, пробуйте.

Matvey
xa110now@yandex.ru

Хочешь увидеть свои советы в журнале? Присылай их на адрес Sklyarov@real.xakep.ru. Ведущий рубрики Tips&Tricks Иван Скляров.

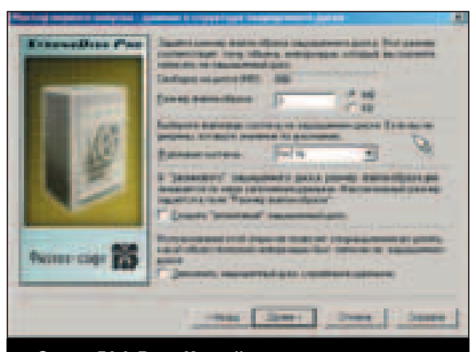
CD ПОД ЗАЩИТОЙ

A.P.$lasH (ap-slash@tfs.kiev.ua)



Strong Disk Pro

Но вернемся к нашим контейнерам. Меня приятно удивила возможность создать "резиновый" диск. Это значит, что пока контейнер пустой, размер файла минимальный (равен размеру заголовка). По мере заполнения зашифрованного диска файл увеличивается. Предельный объем ты можешь указать в поле "Размер



Strong Disk Pro - Контейнерных дел мастер

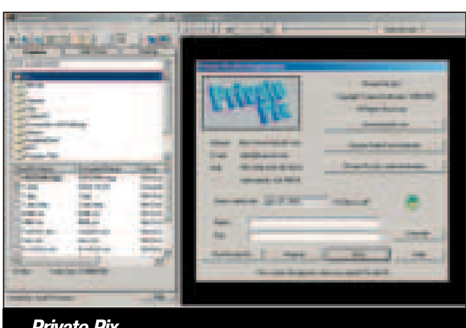
файла-образа". По количеству поддерживаемых алгоритмов Strong Disk обскакал всех предыдущих оппонентов - из предлагаемого набора можно выбрать 3DES, CAST-128, SAFER, Blowfish, AES и Blowfish-448. Более того, заголовок и данные можно зашифровать с использованием разных алгоритмов (по умолчанию программа предлагает оптимальные по скорости и степени защищенности). Новый диск доступен сразу же после форматирования. Кстати говоря, на этот раз обошлось без стандартного диалога винды - Strong Disk форматирует контейнер самостоятельно. Еще одна интересная возможность - на каждом диске по умолчанию создается папка Startup, в которую можно поместить программы для последующей автозагрузки. Открывай в меню Strong Disk пункт "Параметры - Общие". Там есть опция "Автозапуск программ при подключении дисков". Это как раз то, о чем я рассказываю. Большую часть времени утилитой можно управлять при помощи двух кнопок на ее лицевой панели - "Подключить" и "Создать". Диски отображаются в виде закладок все в том же окошке. Специально для лихих и бесстрашных бойцов программа позволяет создавать "ложные" диски. К примеру, приезжает обиженная дивизия на БТРах и начинает живо интересоваться твоими контейнерами. Ты вводишь особый пароль и, расширяя зрачки от восторга, начинаешь демонстрировать открывшиеся в проводнике фотографии телепузиков. Дело в том, что в этот момент настоящие диски подменяются ложными, а оригиналы быстренько испаряются без возможности восстановления. За что тебя потом "расчехлят" из гаубицы - за любовь к телепузикам или за попытку объегорить опечалившуюся дивизию, это уже не суть. Strong Disk предлагает тебе шанс, которым грех не воспользоваться.

Strong Disk Pro
http://www.strongdisk.ru

Ссылка на закачку
http://www.strongdisk.ru/free/sdprorusd.exe

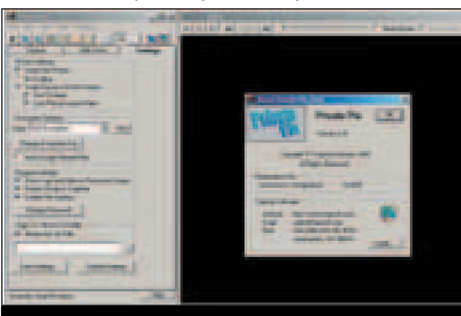
Документация
http://www.strongdisk.ru/free/sdprodoc.zip

<Private Pix>



Private Pix

Последняя программа в этом обзоре о контейнерах ни разу не слышала и компакты записывать не пыталась. У нее своя политика партии - Private Pix умеет шифровать изображения и предоставляет встроенную оболочку для их просмотра. Картинная галерея "Студентки на картошке (Картошка в восторге)" легко превращается в бред сивой кобылы - сплошной набор псевдографики. По крайней мере, именно ее будет вынужден лицезреть коварный извращенец, рискнувший проникнуть в твой компьютер. Бедный мальчик, он не любил синематограф. Ты горько вздохнешь, запустишь Private Pix, и она с радостью покажет тебе, как Маша, Даша и Дуняша наматывают круги по картофельному полю, стегая полотенцами корову из массовки. Но это лирика. Переходим к практике.



Private Pix - Параметры

На самом деле программа не ограничивает себя одними лишь фотографиями. На дворе 21 век. Сверхсекретные досье и бесстыжие фотографии можно хранить во многих форматах. Private Pix понимает JPG, GIF, BMP, ICO, WMF, RLE, и EMF, а также AVI, MOV, MPG/MPEG, MP3, MP2, WAV, MID, RMI, и ASF. Вот такая вот вереница. А что, неприличные мидяхи тоже встречаются. Особенно когда соло-партию Эминема пытаются повторить на тромбоне. Так вот, пришла пора познакомиться с исполняемым файлом программы. Private Pix состоит из двух окон. Слева - браузер, меню и все настройки, справа - область для просмотра изображений + панель управления встроенным проигрывателем. Зашифровать файл - дело нескольких секунд. Находишь его в браузере, выделяешь курсором и выбираешь в меню File - Encrypt File (Файл - Зашифровать файл). Как вариант, ищешь на панели инструментов одноименную кнопку или нажимаешь комбинацию Ctr+E.

При этом браузер одновременно показывает в списке настоящее имя файла и ту абракадабру, в которую оно превратилось по милости Private Pix. Кстати, не пытайся переименовать зашифрованные файлы. Она этого не любит.

Диск программа не трогает, расшифровка всех данных происходит в памяти. На закладке Slide Show расположены параметры отображения слайдов (тут перевод не нужен, верно?), а также краткое руководство по управлению этим процессом с клавиатуры. В разделе Settings можно попытаться уговорить программу вести себя так, как этого хочешь ты. К примеру, сменить алгоритм шифрования. В незарегистрированной версии их всего два - Fast Encryption и Media Stealth, но разве этого мало? Больше - уже экзотика. Шифруем любимую подборку фотографий, хватаем болванку и работаем кнопками. Не забудь переписать на компакт Private Pix. Да, это не IrfanView, но тут уж ничего не поделаешь.

Разумеется, подобных утилит в Сети бесчисленное множество, но на этот раз мне попались именно эти, причем я нисколько не жалею. Программы достойные, свое дело знают. Dekart Private Disk Light вызывает уважение своими размерами и отличным интерфейсом. Это действительно утилита, а не компьютерный офис параноика. Best Crypt с его классической аккуратностью добавляет массу полезных возможностей, являясь, по сути, более продвинутым вариантом PDL. CDLock пригодится тем, кто постоянно торопится и предпочитает защищать свои секреты двумя-тремя взмахами мышиного провода. Strong Disk Pro - находка для настоящего Штирлица. Впрочем, русскоязычный интерфейс и аналогичная справка могут привлечь и более широкий круг пользователей. Private Pix подойдет всем тем, кто чувствует в себе тягу к прекрасному - приватным галереям и немецким фильмам про любовь. Прикинь, что нужно именно тебе. В твоем распоряжении богатый выбор инструментов.

Private Pix
http://www.tropsoft.com

Ссылка на закачку
http://www.tropsoft.com/privpixd.exe

Skylord (sky_lord@mail.ru)

E-BOOK С АНТЕННОЙ

ЧТЕНИЕ КНИГ С ЭКРАНА ТЕЛЕФОНА

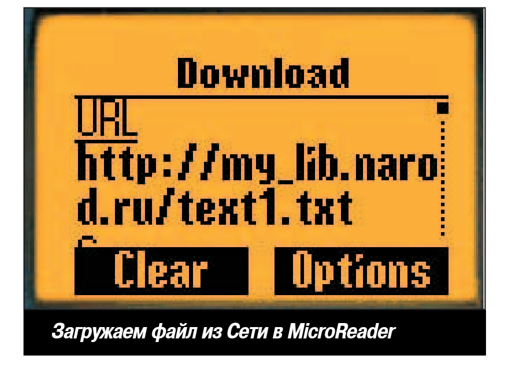
Чтение книг - занятие, безусловно, полезное. Но стандартные бумажные талмуды - это уже прошлый век, ведь в Сети есть все, начиная с романов и повестей и заканчивая учебниками со шпаргалками. А самое главное, что все эти сокровища вполне доступны с обычного мобильника! Тебе не нужен дорогой КПК! Не надо больше таскать с собой килограммы бумаги! Средством образования станет твой телефон: забудь про SMS и звонки и сделай из него настоящую электронную библиотеку!

<Классика жанра>

В одной из статей апрельского номера][мы подробно разбирали, что такое Java в телефонах и какой от нее прок (так что если тебе что-либо будет непонятно в этом материале – постарайся для начала найти и прочесть тот). Напомню, что речь тогда шла в том числе и о чтении текстов, а в качестве основной «читалки» я предлагал использовать мидлет MicroReader. Но если в прошлый раз я отделался общими фразами, то теперь постараюсь поподробнее рассказать об этой замечательной проге. Кстати, перво-наперво стоит убедиться, что у тебя версия мидлета 1.1 - предыдущие версии, лежащие на многих сайтах, не имеют тех фишечек, которые нам нужны. Да, чуть не забыл! В качестве примера я снова буду приводить мои любимые телефоны Siemens, хотя никаких принципиальных отличий у той же Nokia быть не должно...

Итак, MicroReader. Пожалуй, главной фишкой этой проги является возможность чтения книжек прямо из Сети! Нет, это не пресловутый WAP, быстро сжирающий деньги при таком его использовании, а простое скачивание текстовых файлов через http, на что уходит совсем немного наличных средств.

Для начала тебе обязательно надо настроить Ява-профили твоей мобилы, чтобы она могла связываться с Сетью: как это делается, ты прочтешь в уже упоминавшемся апрельском номере][. Когда закончишь со всеми настройками, размести где-нибудь на бесплатном хостинге нужные тебе тексты в обычном формате txt, либо найди сетевую библиотеку, где они лежат в таком виде. В принципе, ты можешь грузить и файлы html, но тогда придется продираться через груду тегов, которые Микроридер, конечно, не понимает. Впрочем, на www.lib.ru, к примеру, html в файлах присутствует только в виде шапки и окончания, а все остальное - обычный текст, так что все сокровища Мошкова в твоем полном распоряжении.



Загружаем файл из Сети в MicroReader

Подготовив объект для чтения, можешь открывать его в мидлете: меню "File", потом "Options" и "Download". В поле "URL", недолго думая, вписывай ссылку на текст. "Save as" - это имя, под которым Микроридер сохранит

его в памяти сотового. А вот следующие два поля - это самое интересное. В "First page" впиши номер страницы, начиная с которой надо загружать текст, а в "# of pages" - размер загружаемого куска (или 0, если хочешь скачать весь файл). Страница в понимании мидлета - это 128 байт, так что ты можешь выбрать столько, сколько поместится у тебя на флекс-драйве. Фантастика, правда?!! Таким образом ты можешь сразу забыть о главной проблеме всех мобил - недостатке свободного места, поскольку любой текст с помощью Микроридера можно вытягивать и читать по частям. Причем когда ты попробуешь осуществить этот финт ушами, то обнаружишь, что в начале каждой части (кроме первой) мидлет заботливо вставляет адрес файла с текстом и номер страницы, с которой начинается эта часть, а в конце - тот же адрес плюс номер последней страницы загруженной части. Тут-то и пригодится еще одна полезная возможность мидлета: он автоматически выхватит ту ссылку, которая сейчас находится на экране и подставит ее в поле "URL" окна "Download". Так что, как только ты дочитаешь очередной кусок текста, можешь сразу и без особых хлопот скачать следующий - останется лишь вписать требуемый номер в поле "First page" и выбрать желаемый размер.

Конец очередной части файла и ссылка на следующую

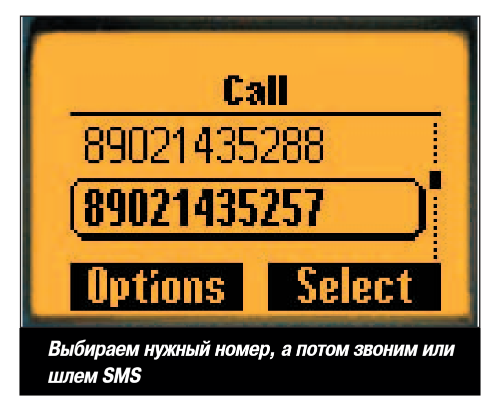
Таким образом легко создавать готовые "списки литературы" со всеми ссылками. А чтобы они были особенно красивыми, посмотри index.txt из комплекта Микроридера (или зацени личный список - http://mjqda.narod.ru/0.txt - редактора «PC Zone») и ты увидишь, как сделать меню для скачивания книги прямо по ее названию.

Еще одно преимущество "полуонлайнового" чтения в том, что не требуется иметь рядом комп. Залил в Сеть кучу книжек и езжай в деревню: достать их ты всегда сможешь, лишь бы там работал твой оператор...

<Побалуемся плюшками>

Этих плюшек у Микроридера - целый вагон. Отдельно хотелось бы отметить две: ведение "записной книжки" и слайд-шоу.

Книжка эта пригодится тебе, если объем (250 записей на SIM-карточке и 50 в памяти телефона) и скромные возможности (всего 3 поля для записи данных абонента!) встроенного телефонного справочника M50 и C55 тебя не устраивают. Хочется хранить телефоны тысячи друзей и знакомых, а к имени каждого написать комментарий, чтобы не забыть, кто это такой?



Выбираем нужный номер, а потом звоним или шлем SMS

Тогда набей на компе и сохрани список абонентов с телефонами и прочей нужной тебе информацией, после чего загрузи этот список в мидлет, и когда на экране появится необходимый номер (помни, что в Микроридере есть поиск, так что долго листать страницы не придется!) - просто нажми кнопку с зеленой трубкой. После утвердительного ответа на появившийся запрос мобила сразу начнет звонить по выбранному телефону. А если ответить на запрос "нет", то появится список всех номеров на этой странице (напоминаю, что страница и здесь - это 128 байт) и предложение либо позвонить, либо отправить на него SMS. Кстати, если нажать "зеленую трубку" когда на странице нет никаких номеров, то мидлет создаст SMS с текстом, который ты в этот момент в нем читаешь - 160 символов, начиная с текущего экрана. Идеальное средство по быстрой рассылке шпаргалок на экзаменах!

Кроме "адресной книги" хотелось бы упомянуть о другой интересной функции - слайд-шоу. Вызывается она из меню "Go to...", и после ее активизации достаточно пару раз пролистнуть страницу в том ритме, в котором ты обычно читаешь, и Микроридер сам начнет листать текст за тебя, избавляя от необходимости использовать для этого большой палец руки (останавливается это слайд-шоу нажатием любой кнопки). Не знаю, как ты, а лично я очень люблю такие вещи - мелочь, а приятно.

На подобном принципе, кстати, работают программы для обучения скорочтению, так что, понемногу увеличивая скорость прокрутки страниц, ты постепенно научишься читать быстрее...

<Ну это просто праздник какой-то!>

А теперь - самая главная вкусность, превращающая чтение книг в Микроридере в сплошное удовольствие. Бравые отечественные программеры в лице Amigo12, не пожалев сил и средств, улучшили

NEXT

Мобила vs КПК

Когда во вступлении я говорил о дороговизне КПК, я немного лукавил. Конечно, модерновый PocketPC или, скажем, Palm Tungsten позволить себе может не каждый, но купить за сотню баксов какой-нибудь Palm III или Palm Vx и приспособить его для чтения книжек вполне реально. Вот и давай разберемся подробнее в плюсах и минусах КПК и мобильников с точки зрения начинающего (или многоопытного) чтеца литературы с экрана.

Главный бонус КПК - дисплей. У младшеньких Палмов он имеет стандартное разрешение 160x160, что позволяет умещать более 30 символов в строке, а самих строк - больше десятка. Экран же типичной мобилы - меньше в разы. Разрешение наших любимых M50/C55 - 101x64. У SL45, S/ME45, S55 побольше - 101x80 (что, кстати, очень положительно влияет на удобство чтения). Но за Палмами в любом случае не угнаться. Однако, в отличие от экранов большинства старых PDA, экран телефона не слепнет на солнечном свету: читать летом на улице что-нибудь с КПКшки практически нереально - только глаза себе портить, ведь не видно там ничего...

Книга на Palm - помещается много, но буквы угловатые...

Фактически, единственный минус небольшого размера экрана мобильника - необходимость часто листать страницы. Но данный "недостаток" нивелируется тем, что листать, в общем-то, довольно удобно: когда держишь в руке M50, большой палец сам ложится на кнопку прокрутки. О C55 (и прочих) с его джойстиком я и не говорю... А если слайд-шоу прикрутить и Microreader+ юзать, то вообще лепота!



Та же книга на C55 - хоть текста и мало, но буковки поаккуратнее выглядят...

Второй естественный вопрос, автоматически вытекающий из первого - размеры самого девайса. Тут, по-моему, какие-либо комментарии излишни: КПК в карман джинсов не сунешь. А если и сунешь, то хорошо от этого не будет ни ему, ни тому, кто помимо него находится внутри джинсов... Мобилу же, как я уже говорил, можно без проблем держать в одной руке, ею же листая страницы. Опять-таки: использовать КПК для чтения шпаргалок на экзаменах у тебя явно не получится, а на мобилу никто и внимания не обратит - подумаешь, с ними сейчас каждый первый ходит... Так что, делай выводы.

А теперь взгляни на проблему с другой стороны: в PDA будет лишь то, что ты сам в него положишь. И если твой путь лежит на черноморские (или иные) побережья или же просто в деревню, то вопрос пополнения запасов книжек может встать со всей остротой. С мобилой нет проблем: берем и скачиваем нужное из Сети. Даже без поддержки GPRS это выйдет совсем недолго и недорого. Конечно, кто-то скажет, что все это глупости, что КПК намного функциональнее обычного телефона... Ну да, не спорю - в чем-то функциональнее. Но и телефон не лыком шит! А кому действительно надо - тот уже купил себе и Пальмы, и Покеты... А мне и мобилы хватает: на ней и читать можно, и звонить, и в игрушки играть... Ну чем не сказка? ;-)

PC_Zone

E-BOOK С АНТЕННОЙ

Skylord (sky_lord@mail.ru)

E-BOOK

Ссылки по теме

1) Родина MicroReader'a
http://home.c2i.net/thvoslef/midlets/MicroReader.html

2) MicroReader+ by Amigo12
http://amigo12.newmail.ru/

3) ReaderC v0.31 by Blade
http://m50j2me.narod.ru/ReaderCv0.31.zip
http://forum.siemens-club.ru/viewtopic.php?TopicID=12451

4) Bookshelf 1.0a by ak1394. Мидлет, похожий на ReaderC (поддерживает сжатие), но с большим количеством возможностей (например, автопереносы слов и слайд-шоу) и более сложной процедурой настройки.
http://bookshelf.freeservers.com

5) TXT2WMLC ver. 1.2a by CheSer software
http://down.gsmsoft.biz/siemens/utilities/txt2wmlc.zip

6) DOC2WMLC by Alexey Sokolov
http://down.gsmsoft.biz/siemens/utilities/doc2wml.rar

7) Онлайновая WAP-библиотека на сайте "Клуб SieMEns 45"
http://wap.o55m.ru

Microreader 1.1 (назвав получившийся продукт "MicroReader+"), в результате чего у программы на 16 Кб увеличился размер, а также появились две ну очень приятных возможности: автоматический перенос слов и более мелкий шрифт. И то и другое в комментариях не нуждается. Посмотри на скриншот и сравни его с остальными: отличия бросаются в глаза. На экране теперь умещается 8 строчек текста, а в строке - 20 букв, причем благодаря переносам пространство экрана используется по максимуму! Одним словом - рулез!

<Если надо сэкономить...>

А сейчас предлагаю обратить пристальное внимание на мидлет-читалку, который в апрельском номере журнала я лишь упомянул - ReaderC v0.31 by Blade. Привлекателен он тем, что работает со сжатыми текстами (ведь JAR файлы мидлета - это, по сути, обычные ZIP-архивы), элегантно решая таким образом уже набившую оскомину проблему нехватки места на флекс-драйве.

Мидлет идет в комплекте со специальным скриптом - swf, облегчающим подготовку его к работе, так что количество необходимых телодвижений сведено к минимуму. Берем текстовый файл (обычный plain text в кодировке Win1251) и прописываем его имя прямо внутри ReaderCv0.32.wsf в качестве значения параметра "opt_file" (он идет сразу после небольшого хелпа в начале скрипта). Для "opt_size" рекомендую брать числа приблизительно в два раза больше количества свободного места на диске мобилы - во столько раз примерно и ужимаются ZIP'ом текстовые файлы.

Теперь запускай модифицированный swf. Он создаст один или несколько (если исходный текст больше "opt_size") каталогов, в которых лежит готовая книжка. Остается скопировать нужный каталог в телефон - и наслаждайся чтением.

На фиг мне Palm, раз у меня такой телефон?

Управлять мидлетом несложно, тем более что и управлять тут особо нечем. Кнопки вверх/вниз листают текст постранично (по окончании очередного 15-килобайтного блока, на которые делится файл в мидлете, автоматически загружается следующий), в меню, вызываемом правой функциональной клавишей, наиболее важные опции - "Bookmark save" и "Bookmark load", позволяющие запоминать и впоследствии восстанавливать позицию чтения. Впрочем, при выходе из мидлета она записывается автоматически, а при следующем чтении сразу восстанавливается...

Одним словом, маленькая (всего 5Кб!), но очень полезная программка. Основной ее недостаток - довольно долгая (примерно секунда) пауза перед показом следующей страницы. Но, по-моему, это не повод, чтобы отказываться от ReaderC. Кстати, в архиве с мидлетом есть и его исходные тексты, так что если ты силен в J2ME, то ничто не мешает тебе исправить баги и усовершенствовать его.

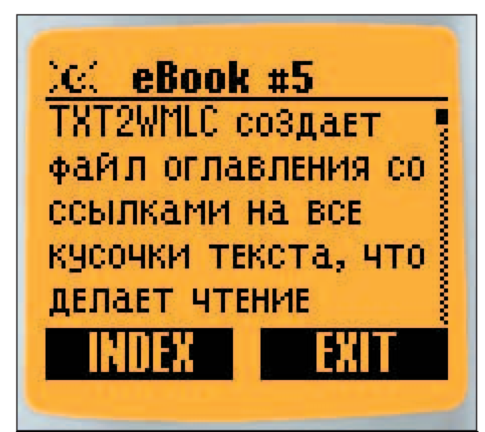
Чтение книги в ReaderC. Роман Стругацких "Гадкие лебеди" размером в 400 Кб целиком уместился на диск Siemens M50 (228 Кб), да еще и место осталось!



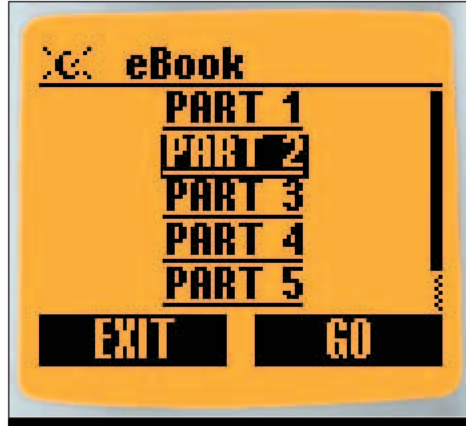
Переходим к закладке в ReaderC...

<Книги через WAP>

Этим методом придется пользоваться, если твой телефон не поддерживает Java, что актуально главным образом для Siemens S/ME45. Лучше всего читать книги в онлайне (например, на wap.o55m.ru), а если это недоступно, то придется сохранять их заранее на диске телефона, для чего необходимо конвертировать текстовый файл в формат WMLC - компилированную страницу на языке WML. Для этих целей можно (и даже нужно) воспользоваться утилитой TXT2WMLC ver. 1.2a by CheSer software. Это, как и в случае с ReaderC, виндовый скрипт, поддержка которых появилась в Win98. Указываешь ему в качестве параметра имя файла и на выходе получаешь либо один wmlc, либо их кучку в созданном подкаталоге, соответствующем исходному тексту. Дело в том, что телефон позволяет загружать WAP-страницы ограниченного объема: например, упомянутые S/ME45 – приблизительно до 2 Кб. А спецификация WML вообще устанавливает предел 1436 байт. К тому же, адекватно воспринимать русские буквы мобила способна только в кодировке UTF-8, так что размер исходного файла увеличивается где-то в 1,5-2 раза. Одним словом, текст надо резать на части.



Текст этой статьи при чтении из WAP'а на телефоне SL45



Выбор нужной части текста в TXT2WMLC

TXT2WMLC создает оглавление со ссылками на все кусочки книги, что облегчает процесс чтения. К сожалению, такой возможности нет у другой интересной программы этого типа - DOC2WMLC by Alexey Sokolov. Она, как понятно из названия, конвертирует в WMLC Вордовые файлы и, что интересно, тоже является VB-скриптом, но для Word: хоть кнопку на панели редактора из нее делай, хоть вообще изменяй внутренности по вкусу. По нажатии на эту самую пресловутую кнопку, в текущем каталоге Word'a (том, что в данный момент появляется в окне "Открыть/Сохранить") создается несколько готовых к употреблению wmlc-файлов. Вот и все, сказать что-либо еще об этом скрипте трудно. Разве что пожелать, чтобы кто-нибудь доделал его до полноценной утилиты.

<Дух Просвещения>

"Учиться, учиться и еще раз учиться", как говорил один небезызвестный исторический деятель. Так последуем же призыву и превратим свой телефон в библиотеку - знания лишними не бывают. Успехов тебе в тяжелом деле самообразования, приятель!

PC_Zone

МАСЯНЯ NON-STOP

МАСЯНЯ NON-STOP

Денис Самарин (densam@densam.ru, www.densam.ru)

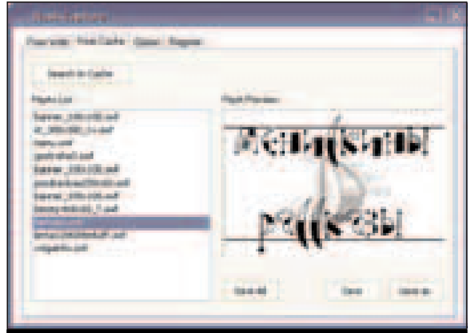


"Пришел, увидел, скачал" - вот девиз настоящего веб-серфера. Красивая картинка? На винт ее! mp3'шка? Туда же! Флешка? Тем более! Стоп. С картинками и mp3'шками проблем нет, а вот скажи мне, как ты обычно скачиваешь флешки? Неужели перекапываешь в их поисках Temporary Internet Files? Надеюсь, что нет. Это ведь так утомительно! Лично я вот в свое время специально побродил по инету, там поспрашивал, тут поглядел, и раскопал, в конце концов, несколько вполне достойных программ-качалок, о которых сейчас и расскажу. Но не думай, что это все, это только присказка! Настоящая сказка тебя ждет во второй части :). Поехали!

ОБЗОР ФЛЕШЕВЫХ КАЧАЛОК И СМОТРЕЛОК В ДВУХ ЧАСТЯХ, БЕЗ ПРОЛОГА И ЭПИЛОГА

Flash Capture

"Добытчик вспышек" обладает поистине замечательными способностями. Это совершенно самостоятельная программа, в отличие от, например, GetFlash которая встраивается в Internet Explorer.



Flash Capture

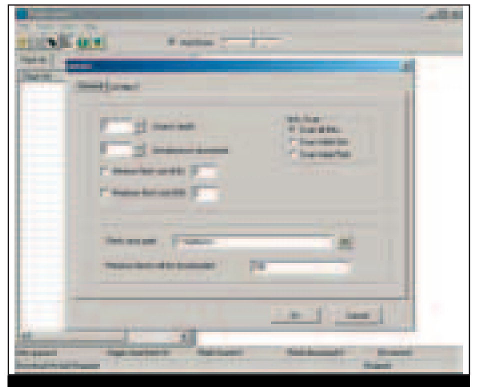
Для того чтобы полностью разобраться в настройках этой утилитки, тебе потребуется потратить какое-то время (секунд десять будет вполне достаточно) и немного пошевелить мозгой (задействовав одну-две извилины, не больше). Короче - более простую прогу найти трудно. И все же несколько комментариев.

Чтобы после скачивания флешки в несколько мегабайт тебе не рыскать во всему винчестеру с истошными воплями: "Куда делся файл? Вы случайно не видели здесь swf'ника?", в закладке "Option" найди поле "Default Flash File Path" (hint: единственное поле в центре большого пустого окна - это оно и есть) и выбери в нем тот путь, куда будут сохраняться файлики. Дальше переходи в закладку "From web", вводи адрес любого сайта и дави на "Go". Просканировав введенный тобой урл, Flash Capture составит список имеющихся на нем флешек, покажет их тебе и предложит сохранить на диск.

Вот и все. А нет, есть еще одно. Дело в том, что когда ты гуляешь по Сети, то все просматриваемые тобой флешки (будь то игрушки или реклама) твой браузер кэширует. А раз так, то зачастую нет смысла заново качать флешку, которую ты уже видел – вполне вероятно, что она на твоей машине уже есть, ее просто надо найти. Эту работу Flash Capture также берет на себя – обрати внимание на закладку "From Cache". Теперь точно все.

Flash Miner

Сразу после загрузки Flash Miner начинает пугать какой-то хитрой регистрацией: программа коннектится на какой-то сайт и делает там что-то непонятное, сигнализируя тебе о процессе с помощью прогресс-бара. Но, в конце концов, прога благополучно запускается.



Flash Miner

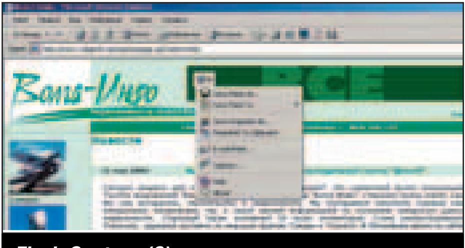
Каких-то принципиальных отличий от Flash Capture Flash Miner не имеет. Но на что я обязательно хочу обратить твое внимание, так это на обилие разнообразных параметров, которые во Flash Capture отсутствуют напрочь. Во-первых, это Search Depth - глубина сканирования сайта. Если, например, этот параметр равен двум, то Flash Miner просканирует не только главную страницу сайта, но и захватит страницы, на которые она ссылается. Дальше - минимальный и максимальный размер скачиваемых флешек. Максимальный, понятное дело, можно и не задавать, а вот ограничение минимального размера реально помогает от захламления винчестера разной требухой типа анимированных кнопочек. Кроме того, имеется параметр, ограничивающий общее количество скачиваемых файлов.

И последнее: если ты задумаешь использовать автоматическое сканирование сайтов, то обязательно побеспокойся о правилах перехода программы по ссылкам. А иначе, если прога "уйдет" по ссылке на другой сайт, ты рискуешь обнаружить у себя на винчестере несколько не то, что ожидал. Для настройки правил перехода существуют параметры "Links Scan" и "Url Filter". Первый определяет, имеет ли Flash Miner право вылезать за границы того сайта, на который ты ее послал, а второй представляет собой набор фильтров, которые позволяют исключить (или наоборот включить) ссылки, соответствующие определенным правилам. Непонятно? Привожу пример. Если в "Url Filter" установить галочку "enable", которую ты обнаружишь в окошке "exclude filter", и ввести слово "banner", то любые линки, содержащие это слово, Flash Miner будет оставлять без внимания.

Таким образом, если Flash Capture – мелкая утилитка для скачивания флешек, то Flash Miner можно назвать офлайновым браузером с узкой специализацией.

GetFlash и Flash Capture

"Мы пойдем другим путем", - заявили программисты из BrotherSoft и создали дополнение к Internet Explorer, позволяющее сохранять flash-ролики как обычные кар-



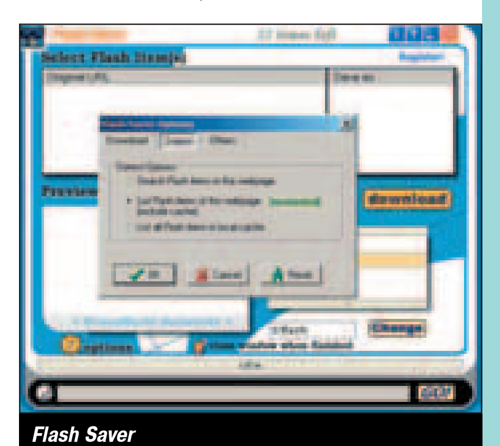
Flash Capture (2)


Get Flash

тинки. После инсталляции Get Flash внедряется в бродилку, и теперь, когда ты увидишь на экране хорошенькую флешечку, и твое сердце сожмется от желания пополнить ею свою коллекцию, тебе достаточно будет щелкнуть правой кнопочкой мышки (вне области Flash-ролика) и выбрать пункт "Save Flash by GetFlash". По тому же самому принципу работает и еще одна утилитка - со знакомым именем Flash Capture (прошу не путать с Flash Capture, описанной выше, я же не виноват, что у разработчиков так слабо с фантазией на названия). Причем работать с Flash Capture 2 (будем называть ее так) мне понравилось даже больше, чем с Get Flash'ем. Как только ты наведешь курсор мышки на любую флеш-картинку, на ней появится квадратик со стрелочкой. Это кнопка вызова меню, с помощью которого ты сможешь сбросить флешку на винч, отослать ее по электронной почте или даже скопировать один фрейм флешки в клипборд.

Flash Saver

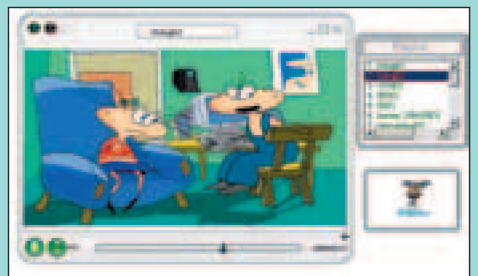
Прежде чем перейти к следующей части обзора, в двух словах расскажу еще об одной проге-«грабилке», которая является некой смесью Flash Capture и GetFlash'а, т.е. умеет добывать swf-файлы разными способами. В софт-каталогах эта прога проходит под кличкой «Flash Saver». Среди ее «особых примет» чаще всего указывают «три режима работы». Режим сканирования конкретного url (как и Flash Capture), сохранение флешек из контекстного меню Internet Explorer'а и поиск флешек на текущей странице сайта (эта функция запускается нажатием клавиши F7).


Flash Saver

Перечитав написанное, я заметил, что, оказывается, ничего не сказал о возможности программ просматривать скачанные флешки. Исправляюсь и сообщаю, что все утилиты, упомянутые выше, не только найдут и сохранят флешку, но и охотно ее тебе продемонстрируют.

Часть вторая: «Смотрелки»

Не вызывает сомнений, что обладание таким мощным арсеналом программ обязательно приведет к тому, что в самое ближайшее время помимо коллекций mp3'шек и avi'шек на твоем компе появится и коллекция swf-файлов. А ведь их тоже нужно чем-то смотреть! Что ты сказал? Стандартный Macromedia Flash Player?! О, мама! Воды, воды... Уф, вроде отпустило. Запомни: никогда не произноси таких слов в обществе приличных людей. Ты бы еще проигрыватель Windows Media вспомнил!


FlashBack

Нет, коллега, куда лучше и элегантнее воспользоваться одним из специализированных плееров. Кстати, предлагаю немного отвлечься. Хочешь, я расскажу, как я вообще на эту тему вышел? Можешь не отвечать, я все равно не слышу. В общем, дело было так. Принес мой старый приятель целый компакт-диск с, как он сам выразился, «прикольными флешинами». Я, разумеется, стал их просматривать, благо дело было на работе, а на работе, как известно "до шести я совершенно свободен". И знаешь, мне довольно быстро надоело каждый раз выполнять одну и ту же примитивную процедуру: открыть файл, начать проигрывание. Вот тут-то я задумался: а ведь есть, наверное, та прога, которая спасет отца русской демократии и станет winAMP'ом в мире флеш-файлов. И такая прога действительно нашлась. Даже две!

Первая называется Flashback, а вторая Softsun Flashplayer. Сразу скажу, что и та, и другая - вполне достойные плееры. Какую из них выберешь ты, зависит исключительно от твоего вкуса. Лично я остановился на обеих. По четным дням использую Flashback, а по нечетным - Softsun Flashplayer.

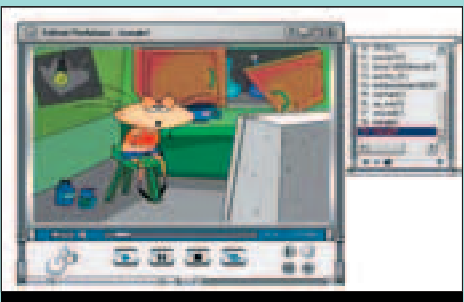
Итак, Flashback. Вся программа разбита на три окошка: окно просмотра, окно предварительного просмотра и playlist. Надо сказать, что за идею одновременного размещения на экране и окна просмотра, и окна предпросмотра авторам можно сразу дать Нобелевскую премию - очень удобно. Пока идет проигрывание одной флешки, можно быстренько в маленьком окошке просмотреть остальные.

Организация работы с плейлистом напоминает WinAMP'овскую. Можно добавлять отдельные файлы (кстати, Flashback понимает как sfw, так и exe'шники), а можно целые каталоги. Кроме того, если нажать кнопочку F3 или выбрать пункт "Search IE Cache", то в playlist добавятся флешки из темповых каталогов (в меню Option выставь параметр IE Cache File more than... больше десяти, чтобы в плейлист не попал всякий флешевый мусор).

Прежде чем начать проигрывать файлы, я советую тебе зайти в меню ZOOM и выставить значение "100%". По какой-то загадочной причине изначально Flashback растягивает изображение так, что флешки маленького формата сильно искажаются.

При проигрывании файлов из списка playlist'а плеер ориентируется на значения трех параметров: Auto Play, MovieLoop ("зацикливание одной флешки) и ListLoop (последовательное "круговое" проигрывание всех файлов). Если с двумя последними все более или менее ясно, то про Auto Play расскажу чуть подробнее. Представь себе, что ты настроил все, как нужно, загрузил в плейлист длинный список файлов, удобно уселся на диван, и вдруг приятный просмотр прекращается, поскольку какой-то умник решил в начале ролика нарисовать кнопку "Start", "Begin" или что-то в этом роде. Так вот, если Auto Play выставлен, то такого рода неприятности тебя обойдут стороной, так как Flashback автоматически пропустит это фрейм!

Что еще умеет Flashback? Ну, например, менять облик с помощью скинов, преобразовывать sfw-файл в exe'шник и переходить к конкретному фрейму флешки (по номеру). И - сюрприз, сюрприз! - Flashback способен изготавливать скринсейверы! Супер, да? Причем делается это буквально нажатием двух клавиш. F4 (или MakeScreensaver из меню) и Enter, чтобы подтвердить название новоиспеченного хранителя экрана. Все! После этого в "Свойствах экрана" в разделе "Заставка" появится новое название.


Softsun Flashplayer

Теперь перейдем ко второму кандидату - Softsun Flashplayer'у. Хоть и говорят, что "повторение - мать учения", я, тем не менее, повторяться не буду, так как Softsun Flashplayer - почти полный аналог Flashback. Все, что умеет Flashback, умеет и Flashplayer, и даже интерфейсы у них очень похожи. Хотя нет, не все. Во Flashplayer'е нет поддержки скинов, и я нигде не нашел, как отключить режим AutoPlay (хотя зачем тебе отключать этот режим – ведь именно его наличие делает эти плееры уникальными?!! Только представь себе – можно просмотреть все мультики о Масяне, ни разу не подойдя к компьютеру, чтобы нажать на кнопку «Старт», с которой у Олега Куваева начинается каждый мульт!)

Зато есть такая модная фича как "Transparent", которая переводит программку (вместе с проигрываемой флешкой!) в полупрозрачный режим. И, кроме того, Flashplayer умеет "грабить" фреймы, на что Flashback, увы, не способен.

Где найти описанный софт?

Flash Capture (shareware, 1.3Мб)
http://flashcapture.zbsoft.net

Flash Capture 2 (shareware, 1.2Мб)
http://www.flashcapture.com

Flash Miner (shareware, 994Кб)
http://www.myminer.com

GetFlash (shareware, 1.172Мб)
http://www.brothersoft.com

Flash Saver (shareware, 1.1Мб)
http://www.downloadatoz.com/flashsaver

Flashback (shareware, 1.01Мб)
http://www.wekasoft.com/flashback

Softsun Flashplayer (shareware, 1.8Мб)
http://www.softsun.com.cn

PC_Zone

ХАКЕРСКИЕ ВОЙНЫ



mindw0rk <mindw0rk@mail.ru>

Самая известная, самая многочисленная и самая авторитетная на протяжении 80-х годов группа Legion of Doom была идолом компьютерного андеграунда. Членство в LoD однозначно говорило о высокой квалификации и, как минимум, вызывало уважение. Хакеры из Legion of Doom вполне могли учинить хаос в любой коммерческой компании, но главным правилом в группе было следование хакерской этике. Каждый мембер специализировался в какой-то области, и сочетание их талантов делало группу еще сильнее. До конца 80-х она была номером один на просторах компьютерного андеграунда, однако вскоре нашлась команда, которая бросила вызов могущественной LoD. Последовавшие события вошли в историю как "Великая хакерская война".



LEGION OF DOOM VS. MASTERS OF DECEPTION

<Legion of Doom>

Хак-группа Knights of Shadow в 1984 году состояла исключительно из известных личностей. Если ты не успел прославиться на олимпе андеграунда, какими бы знаниями ты ни обладал, путь в нее для тебя был закрыт. Lex Luthor'а знали многие. Несмотря на свой юный возраст, он уже успел проникнуть в несколько сложных систем и на фрикерских BBS пользовался авторитетом знающего человека. Поэтому, когда Lex попросился в KoS - остальные мемберы не стали возражать. Тусуясь на разных бордах, Lex Luthor познакомился со многими хакерами. На досках, подобных Plovernet и Osuny, можно было встретить специалистов всех мастей. Чтобы расширить общие знания в группе, Lex предложил парням из KoS зачислить в коллектив нескольких его друзей, имеющих отличную квалификацию. Но, несмотря на все доводы, ему отказали. У кандидатов действительно имелись хорошие знания, но звездами они не были, громких подвигов не совершали, так что места для них не нашлось. Такая идеология разозлила Lex'а, и он решил оставить группу, чтобы сформировать свою. Такую, где будет цениться не сомнительная популярность, а знания и умения человека.

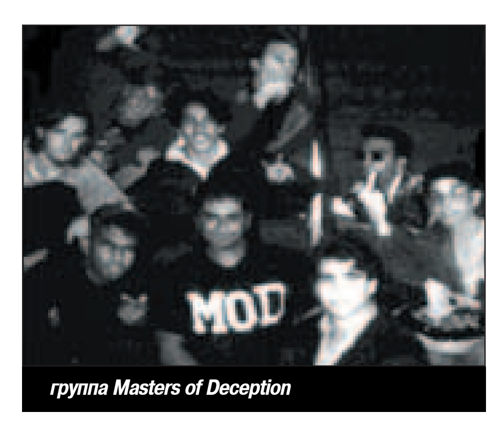
В том же 1984 году Lex запустил новую BBS'ку Legion of Doom и попутно принялся сколачивать команду с одноименным названием. Имя группы взялось не от фонаря - в начале 80-х по телевизору часто крутили мультсериал "Superfriends", в котором главный злодей Lex Luthor возглавлял банду Legion of Doom, всячески строившую козни героям. Этот антигерой был своего рода кумиром для хакера. Основной костяк команды набрался из Plovernet - в то время центровой андеграундной борды. В основном в группу вошли ближайшие друзья Lex'а плюс несколько просто хорошо зарекомендовавших себя парней. Первоначальный состав выглядел так: Lex Luthor, Karl Marx, Mark Tabas, Agrajag the Prolonged, King Blotto, Blue Archer, EBA, The Dragyn, Unknown Soldier. На протяжении следующих десяти лет он много раз менялся - одни приходили, другие уходили. В какой-то момент группа разделилась на две: Legion of Doom, которую составляли по большей части опытные фрикеры, и Legion of Hackers, члены которой занимались компьютерным взломом. Когда все мемберы стали хакерами, две разрозненные команды опять соединились в одну - LoD. С 1985 года ее лидером стал Erik Bloodaxe (Крис Гагганс), занимавшийся организаторскими вопросами и приводивший большинство новых людей. Судьба кандидатов решалась путем голосования остальных мемберов.

Благодаря хорошо организованной структуре, группа принимала активное участие в развитии компьютерного андеграунда. Члены LoD часто выпускали security-документацию, проводили всевозможные тусовки, они же были основным источником новостей хакерского мира. А Legion of Doom BBS вскоре стала самым большим в мире архивом информации хакерской тематики. Мегабайты текстов хранились на винте борды, но доступ к ним имели лишь избранные. Несмотря на известность самой группы, ее хакерская деятельность оставалась в тени. Активные мемберы избегали славы и обсуждали свои проекты исключительно в закрытых от посторонних местах. В связи с этим очень скоро вокруг LoD возник мистический ореол. Как только ее ни называли: и "организованная группа кибертеррористов", и "банда подростков, сформированная для уничтожения сервиса 911", и даже "коммунистическая угроза национальной безопасности". Если непослушных маленьких детей родители пугали всякими чудовищами, у системных администраторов настоящий ужас вызывала перспектива стать жертвой Legion of Doom. Но несмотря на то, что хакеры LoD на протяжении 80-х проникли в десятки тысяч самых разных систем, практически всегда посещение мотивировалось лишь исследовательским любопытством. Взломщики тихо приходили, тихо скачивали интересующую их информацию и так же тихо уходили, заметая следы. Были и исключения - некоторые мемберы злоупотребляли своими знаниями и нарушали главное правило: "Не навреди". Таких было немного, и LoD старалась избавиться от них как можно быстрее (например, в конце 1985 из группы был изгнан Terminal Man, который стер в одной из систем важную информацию).

То, что внутри хакерской команды разделялось на "можно" и "нельзя", у федералов проходило под однозначным приговором "виновен", только с разными сроками. За любовь к исследованиям поплатились многие хакеры LoD: X-Man, Unknown Soldier, Sharp Razor, The Mentor, Bill from RNOC, Thomas Covenant, The Prophet, The Leftist, Urvile и другие. Практически каждый из сорока членов группы, если вовремя не завязывал со своей деятельностью, рано или поздно оказывался под колпаком.

<Masters of Deception>

В 1989 году, просматривая постинги на фрикерских BBS, Erik Bloodaxe заметил, что какой-то парень подписывается: "Phiber Optik of the LoD". Быстро вычислив номер телефона самозванца, Erik позвонил ему домой и поинтересовался, какого дьявола тот говорит о своей причаст-



группа Masters of Deception



Mark Abene aka Phiber Optik

ности к группе. "Потому что я и есть член группы", - спокойно заметил Phiber Optik (настоящее имя: Mark Abene). Лидер LoD пояснил Марку, что вступить можно только с разрешения активных мемберов и при наличии определенной квалификации. Но едва зашел разговор на технические темы, Erik понял, что по уровню знаний этот парень опережает многих его товарищей. Phiber Optik был экспертом по телефонным сетям и мог вытворять с ними что угодно. А помимо этого, был опытным хакером. И это при том, что парню едва исполнилось 17 лет. Конец разговора резко отличался от начала - Erik Bloodaxe пообещал обсудить кандидатуру Марка со своими друзьями, и через несколько дней Phiber Optik уже официально присоединился к Legion of Doom.

Но спустя всего несколько недель некоторые мемберы LoD стали сожалеть о принятом решении. Оказалось, у Марка не только неординарные мозги, но и не абы какое самолюбие вкупе с наглостью. Его сообщения на форумах были полны бахвальства, а некоторые поступки компрометировали всю группу. Поэтому не прошло и полгода, как талантливого новичка попросили вон.

Phiber Optik в 1989 г. уже был довольно известен, а среди хакеров Нью-Йорка вообще считался легендарной личностью. Тут у него было много друзей, и, покинув LoD, он стал подумывать над созданием своей группы. Название предложил Пол Стайра - преуспевающий студент престижного колледжа, а по совместительству начинающий хакер Scorpion, с которым Марк познакомился за полгода до этого. Слово MoD было намеком на то, что новая группа хакеров на шаг впереди LoD. Собираясь вместе, члены будущей команды Masters of Deception ставили конкретную цель - вытеснить Legion of Doom с пьедестала славы и обрести титул хакерской группы номер один. Состав группы выглядел так: Phiber Optik, Scorpion, HAC, The Wing, Acid Phreak, The Seeker, Lord Micro, Red Knight, Corrupt, Outlaw.

Большинство мемберов MoD особо не заботились о принципах хакерской этики. Деяний одних только The Wing и Outlaw хватало, чтобы обеспечить всех пожизненными сроками. Но если раньше взломщики направляли свою энергию на беспомощные серверы правительственных и коммерческих компьютеров, то с начала 1990 года их новой целью стала группа Legion of Doom.

<Война компьютерных умов>

В первые месяцы после рождения Masters of Deception явных стычек между MoD и LoD не было. Группы нередко пересекались на BBS, не отказывая себе в удовольствии подпокалывать друг друга. Все началось с того, что однажды в разгар болтовни между шестерыми членами Legion of Doom на закрытой телеконференции появился чужак. "Yo, dis is Dope Fiend from MoD", - прозвучал громкий голос, прерывая беседу хакеров на полуслове. В ответ тут же раздалось: "Выкиньте кто-нибудь этого ниггера с линии!" Автор заявления не знал, что на самом деле гостем был Corrupt - единственный чернокожий мембер Masters of Deception, болезненно воспринимающий любые проявления расизма. И уж тем более презрительное "ниггер" в свой адрес.

Ответный удар не заставил себя долго ждать. Джон Ли (настоящее имя Corrupt'а) быстро нашел домашний телефон Erik'а Bloodaxe'а - лидера LoD - и засыпал его издевательскими посланиями. Телефон в квартире Криса звонил постоянно, не помогали ни уговоры, ни угрозы, ни вешанья трубки. Хакер даже не мог понять, зачем и почему его достают, так как в тот злополучный день не сидел в конференции. Узнав, что его мучители - парни из MoD, Erik Bloodaxe решил их проучить. В это время в сети как раз появилась написанная Acid Phreak'ом история рождения группы Masters of Deception. Крис ее подредактировал, переписав с использованием словечек типа "braza", "de gut", "what's up" и т.п., понатыкал в текст выражение «k001 x@цk3r$k13» и в таком виде растиражировал в публичных местах. Выглядело это так, будто кучка ламеров решила рассказать о своем величии. Для членов MoD, не ожидавших такого коварства, это был удар ниже пояса. Открытое объявление войны.

Некогда безобидные подколки на BBS быстро превратились в яростный флейм. Обвиняя друг друга в ламерстве и прочих грехах, хакеры не упускали возможности продемонстрировать это на практике. Они применяли все свои знания и изобретательность, атакуя вражеские телефоны и компьютеры. То и дело у одного из членов той или иной группы телефон переводился в режим таксофона, а система давала сбой. Хранить файлы внутри компьютера стало небезопасно. Как и разговаривать по телефону - линии постоянно прослушивались.

Идея стать лучшей хакерской группой к этому времени окончательно завладела MoD. Команда Phiber Optik'а старалась осуществить как можно больше крупных взломов, для поднятия авторитета выбирались самые сложные системы. Legion of Doom была не в восторге от происходящего и просто огрызалась на нападки своих недругов. В то же время Masters of Deception искала новые изощренные способы им досадить. Весной 1991 Erik'у Bloodaxe'у даже пришлось обратиться в ФБР, так как хакеры MoD поставили на прослушивание закрытую телефонную линию его security-фирмы Comsec. Клиенты вряд ли были бы в восторге, что security-эксперты, которым они доверили свою безопасность, допустили проникновение посторонних в телефонную сеть. Но заявление Криса об активности хакерской группы не стало для федералов неожиданностью. Как оказалось, те уже давно следили за назойливыми хакерами. Арест всей банды был лишь делом времени.

Несмотря на многочисленные улики, собранные за несколько месяцев, до суда дело компьютерных взломщиков дошло только в июле 1992 г. Членов MoD обвинили по 11 пунктам, "стоящим" по 5 лет тюрьмы и $250000 штрафа. Но то ли благодаря хорошему адвокату, то ли неким смягчающим обстоятельствам, каждый получил не больше года.

Legion of Doom просуществовала вплоть до 1994 г. В это время отошли от хакерского сообщества немногие оставшиеся мемберы, и некогда могущественная группа просто исчезла, оставшись, впрочем, в памяти пионеров тех времен и став неотъемлемой частью истории - одной из самых известных легенд компьютерного андеграунда.



PC_Zone

PHIBER OPTIK: ПОВЕЛИТЕЛЬ ТЕЛЕФОННЫХ СЕТЕЙ.

mindw0rk <mindw0rk@mail.ru>



HACKER'S HALL OF FAME # 7

Когда в 1990 г. журнал "Harper" организовал на своем сервере общедоступный форум, посвященный компьютерной безопасности, поучаствовать в дискуссии зашли многие компьютерные эксперты и хакеры. Две противоборствующие стороны столкнулись лицом к лицу. Большинство участников придерживались установленных на форуме правил и относились к оппонентам с уважением, но были и такие, кто, не стесняясь в выражениях, публично высказывал о противниках все, что о них думает. Яростней всех нападал на хакеров Джон Пэрри Бэрлоу - независимый security-консультант, питающий к компьютерным взломщикам особую нелюбовь. В одном из его постингов говорилось, что основное различие между хакерами - не уровень их знаний, а уровень их психической неуравновешенности. "Заберите у них модемы, дайте в руки скейтборды, и не будет даже видно особых перемен". Всего через 13 минут после того, как это сообщение появилось на форуме, последовал ответ. Размещенное ниже письмо включало все сведения о кредитной карточке Джона Пэрри, информацию о владельце, его контакты, место работы и некоторые другие конфиденциальные данные. В конце мессаги стояла скромная подпись - Phiber Optik.

<Детство юного гения>

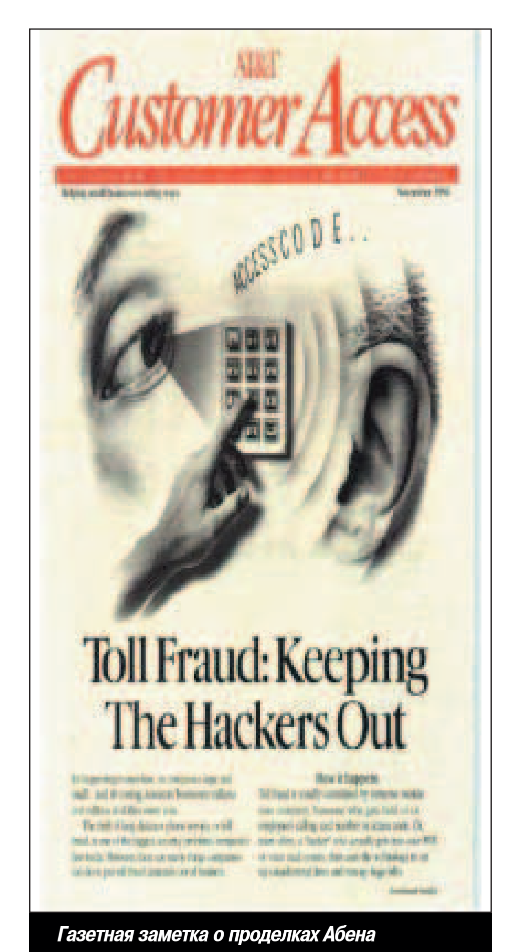
Когда у Чарльза и Глории Абен в 1972 г. родился сын, они уже в первые месяцы заметили, что их ребенок опережает в развитии своих сверстников. В 2 года Марк уже знал весь алфавит и, еще толком не умея держать карандаш, пытался писать слова. Три года спустя он уже вовсю читал книжки, причем не какие-нибудь сказки, а сложные технические издания. Конечно, многих вещей Марк не понимал, но старался разобраться в каждом неясном моменте, постоянно обращаясь с вопросами к родителям. Чарльз и Глория только разводили руками - их чадо интересовалось такими сложными вещами, что даже они не могли ему помочь. С самого рождения Марк тянулся к технике.

Когда Марку исполнилось восемь, знакомый матери, часто заходивший в гости и заметивший большой интерес смышленого паренька к радиоэлектронике, подарил ему книжку "Using Electronics". Это была старенькая, давно не переиздававшаяся брошюра, но для юного электрика она стала своего рода наставником. В ней были приведены схемы разных устройств. Марк сразу же загорелся новой идеей – он решил самостоятельно собрать настоящий радиоприемник. Для этого требовались кое-какие детали, и, занимаясь их поисками, он открыл для себя магазины Radio Shack. Там продавалось все - от моторов до микропроцессоров. Марка поразило такое изобилие, и эта сеть магазинов на долгие годы приобрела в его лице постоянного посетителя.

Помимо выдающегося интеллекта и интуиции у парня обнаружилась феноменальная память. Он мог почти дословно пересказать прочитанный отрывок размером в несколько страниц, помнил сотни телефонных номеров. К десяти годам телефоны для Марка стали значить больше, нежели просто средство связи, используемое с целью поболтать. Он уже долгое время занимался тем, что набирал случайные номера и общался с незнакомыми людьми, пытаясь узнать у них что-нибудь интересное. Но настал момент, когда самым интересным для него стало узнать, как работает телефонная система. Что происходит там внутри.

<Секреты Ma Bell>

Достать нужную информацию было не так-то просто. Марк проводил много времени в библиотеках, но ничего конкретного о принципе действия сетей Ma Bell найти не мог. Где-то рядом на улицах Нью-Йорка кипела фрикерская жизнь - сотни молодых парней дружно исследовали просторы Ma Bell и осуществляли дерзкие пранки. Но Марк даже не подозревал, что кроме него еще кто-то мог так же сильно интересоваться внутренним устройством телефонов. Рассчитывать он мог только на себя. Следующие несколько лет Марк Абен постигал секреты Bell как увлекательную головоломку. У него не было абсолютно никаких советчиков или документации - ничего, что могло помочь. Методом тыка, путем экспериментов и догадок он осваивал премудрости, которые публикова-


AT&T Customer Access

ACCESS CODE...

Toll Fraud: Keeping The Hackers Out

Газетная заметка о проделках Абена

лись в журнале TAP и которыми обменивались между собой фрикеры. У него не было той базы знаний, которую успели собрать телефонные взломщики, но не было и зависимости от нее - Марк творчески подходил к поиску информации и часто выяснял такие вещи, о которых не знали даже более опытные "коллеги".
В 11 лет Марк Абен впервые увидел компьютер. Некоторые магазины устанавливали у себя первые персоналки, чтобы привлечь клиентов. Сказать, что Марка привлекла новая игрушка - значит, не сказать ничего. Сбегая со школьных занятий, он целыми днями околачивался в нью-йоркских супермаркетах, дожидаясь, когда место за TI-994A или Apple][s будет пустовать. А потом садился за клавиатуру и уже проверенным методом тыка пытался разобраться в том, как оно там все работает. Изучение компьютеров давалось Марку легко. Он быстро освоил Basic и уже скоро писал на нем первые программы. Конечно, большой соблазн представляли игры, и паренек не отказывал себе в удовольствии порубиться во что-нибудь типа Elevator Action или Jungle Hunt.

<Phiber Optik>

Видя сильное увлечение сына компьютерами, родители купили ему на Рождество TRS-80 - популярную недорогую модель с 4 Кб ОЗУ на борту. Спустя год память компа расширилась до 20 килобайт, а рядом с клавиатурой появился 300-бодовый модем. В это время большой популярностью пользовалась Compuserve - коммерческая система, пользователи которой могли общаться друг с другом в конференциях и чатах. Попав в онлайновую тусовку компьютерщиков, Марк, наконец, нашел единомышленников и окунулся в виртуальный мир с головой. Даже недолгое пользование Compuserv'ом стоило денег, а юный фрикер находился в онлайне постоянно. Поэтому первый же счет вызвал шок у родителей. Чаты на этом закончились, но незадолго до отключения Марк успел узнать несколько телефонов станций BBS.
На андеграундовые борды он наткнулся не сразу, а когда это произошло - необходимость в остальных сразу отпала. Шел 1985 год - расцвет хакерского сообщества, но для Марка все только начиналось. В этом году он увидел "WarGames", в этом же году совершил свой первый взлом университетской сети в Лонг-Айленде. Затем взломы последовали один за другим. Марк не останавливался подолгу в одной системе. Работая по ночам, он постоянно искал новые полигоны для исследований и состязаний.
По мере того как повышалась его квалификация, Абен стал потихоньку втягиваться в андерграундную тусовку. Ему удалось познакомиться с лучшими фрикерами Нью-Йорка, и все вместе они нередко собирались для проведения фрикерских рейдов. В их среде Марк был известен под именем Phiber Optik.
Основным объектом исследований Марка оставалась Ma Bell. К 17 годам он мог вытворять в телефонных сетях все что угодно: от блокировки номеров до отслеживания звонков. Последнее, кстати, было его любимым занятием. Phiber обожал узнавать о людях тщательно скрываемые факты и вываливать их перед ними, любуясь реакцией. На собственной шкуре эту любовь ощутили многие знаменитости (например, Джулия Робертс). В хакерском мире известность Phiber Optik получил благодаря своим постингам на авторитетных BBS. Он с удовольствием отвечал на все вопросы, а если видел в письмах других ошибки, обязательно их комментировал и поправлял. Весть о хакере, "который все знает", быстро облетела компьютерный андеграунд. Кто он такой? Откуда? В каких системах он успел побывать? Мало кто об этом знал, но какая на самом деле разница? Главное, что этот парень определенно относился к элите.

<Звезда СМИ>

Весной 1989 г. Phiber Optik присоединился к Legion of Doom. Причастность к столь известной хакерской группе прославила его еще больше, а славу Марк любил. Впрочем, продлилось членство в LoD недолго. Из-за конфликтов с остальными мемберами, особенно с Erik'ом Bloodaxe'ом, ему пришлось выйти из состава группы. Но уже несколько недель спустя появилась Masters of Deception. Несмотря на то, что Phiber Optik официально считался создателем группы, он никогда не принимал активного участия в ее жизни. Война с LoD по большей мере прошла мимо него - он просто контактировал с остальными мемберами и помогал им в разных вопросах.
В это время Марк работал в небольшой фирме, занимаясь ремонтом персональных компьютеров.
Его не слишком интересовали военные или какие-то top-secret объекты - гораздо больше он любил мощные мейнфреймы. Проникая на них со своей маленькой персоналки, Phiber Optik наслаждался свободой, которую давали мощь и совершенство этих больших машин.
В конце 80-х в СМИ произошел всплеск интереса к хакерам. Репортеры искали героя, который бы воплощал все качества компьютерного взломщика, был известен в узких кругах и мог поделиться своими секретами. Большинство представителей андеграунда не собирались выходить из тени, но Марк был совсем не против того, чтобы стать звездой. Статьи о Phiber Optik'е появились в New York Times, NY Newsday и многих других популярных изданиях. Он принял участие в телевизионном шоу, посвященном хакерам, а по количеству выступлений на радио "Off The Hook" Абену не было равных. Марк стал любимцем журналистов - он свободно держался перед камерой и мог часами рассказывать свои истории, пропитанные духом хакерской этики.


Phiber Optik за работой :)

Apple][

<Кумир молодежи>

В декабре 1980 г. к разговорчивому хакеру впервые наведались правоохранительные органы. Доказательств причастности Марка к какому-либо инциденту у них не было, поэтому они ограничились тем, что конфисковали все его компьютерное оборудование. Следующий визит был нанесен год спустя и оказался намного серьезнее. В 11 утра в комнату спящего хакера ворвались сотрудники ФБР и Секретных Служб, приставили пистолет к его голове и увезли в участок. На этот раз у федералов были кое-какие улики, но так как Марк был еще несовершеннолетним и провинностей ранее не имел, все, что можно было сделать - это привлечь его к общественным работам.
Отработав положенное, Марк Абен устроился на работу в Echo - один из первых интернет-провайдеров. К этому времени он решил завязать со своим прошлым и подумывал о том, чтобы построить карьеру. Работа системным администратором и консультантом в Echo приносила удовольствие, и Марк отлично с ней справлялся, за что даже получил повышение зарплаты. Но так просто оставлять его в покое федералы не собирались.
В январе 1994 г. Phiber Optik'а снова арестовали. Секретные Службы два года собирали информацию о деяниях хакеров из Masters of Deception. Их дело занимало толстую папку, в которой находились жалобы от разных телефонных компаний и коммерческих организаций. MoD стала козлом отпущения для многих фирм, ставших жертвами хакеров. Уже совершеннолетние парни теперь не могли отмазаться так просто. Первыми отсиживать 6-месячный срок в тюрьму отправились Acid Phreak и Scorpion. Следующим был Марк. Объявляя приговор, судья сообщил, что хакер Phiber Optik будет для остальных подростков примером того, куда могут завести хакерские игры. Марк Абен получил год тюрьмы.
Дело Phiber Optik'а освещалось во всех основных СМИ. Многие журналисты и телевизионщики навещали его в тюрьме. Марк действительно стал примером, но не тем, о котором говорил судья, а примером для подражания. Для тысяч молодых ребят, прочитавших в газетах историю заключенного хакера, он стал кумиром. Они принялись изучать компьютерную безопасность, становясь на путь хакерства. В 1995 г. в честь получившего, наконец, свободу Phiber Optik'а состоялась большая вечеринка, на которую съехались многие хакеры и фрикеры со всех концов Америки. Чуть позже журнал "New York magazine" включил Марка Абена в список ста умнейших жителей Нью-Йорка. Сейчас бывший хакер возглавляет свою маленькую фирму из трех человек "Crossbar Security" (http://www.crossbar.com), специализирующуюся на консультациях в сфере inet security.

КОМПЬЮТЕР БУДУЩЕГО

Елманов Олег (SpyDr@comail.ru)



Компьютер будущего

Думаю, ты неплохо разбираешься в женской красоте и без труда отыщешь в толпе красивую девушку. А можешь написать программку, которая бы сама отбирала симпатюль по фотографиям, например, на сайте знакомств? А по каким критериям ты их будешь отбирать? Даже самый мощный компьютер с традиционной архитектурой вряд ли справится с такой задачей. Здесь на помощь приходят нейросетевые технологии. Слышал про такие? Что-то из фантастики и "Матрицы"? Я тоже так подумал, когда в первый раз про них услышал.

Что такое нейрокомпьютер и на что он способен

Что такое нейрокомпьютер

В последнее время все чаще можно услышать слова "нейронная сеть", "нейрокомпьютер". Как ни странно, многие уже сталкивались в повседневной жизни с их работой. Системы распознавания текста, устройства считывания штрих-кода, голосовое управление, "умная" бытовая техника и многое другое.

С формальной точки зрения, нейронная сеть - это параллельная связная сеть простых элементов - нейронов, которая взаимодействует с объектом реального мира аналогично биологической нервной системе. Ее программная или аппаратная реализация называется нейрокомпьютером.
Непонятно? Тогда с самого начала.

Немного биологии

Человеческий мозг содержит порядка миллиарда вычислительных элементов, называемых нейронами. Нейроны связаны между собой. Эта сеть нейронов отвечает за все явления, которые мы называем мыслями, эмоциями, познанием и т.д.



Строение биологического нейрона

Скорость передачи нервных импульсов между нейронами сравнительно мала, но, несмотря на это, скорость обработки информации в коре мозга огромна. Это достигается за счет того, что внешняя информация распределяется по всем нейронам и обрабатывается ими одновременно, то есть реализуется максимально распараллеленная обработка распределенной информации.
Если тебя заинтересовал состав нейронов, их типы, функции и принципы работы, на досуге зайди в библиотеку и поройся в медицинских справочниках. Там ты точно найдешь много полезного.

Так все же, что это такое?

Как ты уже догадался, нейронная сеть состоит из нейронов, соединенных между собой. Искусственный нейрон имитирует в первом приближении свойства и работу своего биологического прототипа.

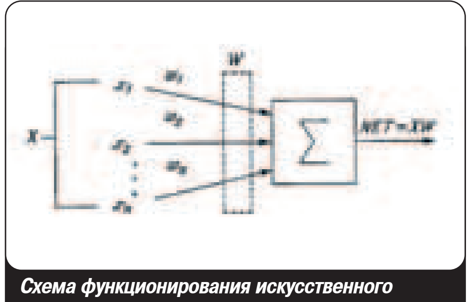
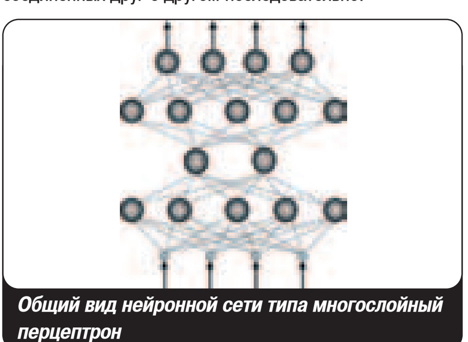


Схема функционирования искусственного нейрона

Общие принципы работы искусственного нейрона можно описать так:
На вход нейрона поступает множество сигналов, выходов других нейронов. Каждый вход характеризуется некото-

Российская инновационная компания "НейрОК" разработала службу ассоциативного поиска документов. Так, нажимая на кнопку "more like this" на портале InfoSeek или "Найти похожие документы" на российском Infoart.ru, получаешь похожие по смыслу документы. Это происходит благодаря нейросетевым программам, обученным распознавать семантику текстов.

рым весовым коэффициентом, определяющим важность поступающей по нему информации. Полученные значения суммируются, преобразуются активационной функцией и поступают на выходы нейрона.
Совокупность нейронов, связанных между собой, образует нейронную сеть. В настоящее время существует более 200 разновидностей нейронных сетей, но основной, самой распространенной и простой является многослойный перцептрон. Он состоит из слоя входных нейронов, слоя выходных нейронов и нескольких внутренних слоев, соединенных друг с другом последовательно.



Общий вид нейронной сети типа многослойный перцептрон

Для того чтобы нейронная сеть начала корректно работать, ее необходимо обучить. Необученная нейросеть не имеет даже "рефлексов" - на любые внешние воздействия ее реакция будет хаотичной. Обучение состоит в многократном предъявлении характерных примеров до тех пор, пока она не станет давать на выходе желаемый отклик.
Существует немало алгоритмов обучения нейросетей, в зависимости от решаемой задачи, типа сети, исходных данных и т.п. Самым распространенным является алгоритм обратного распространения ошибки. Его принцип в следующем: Есть некий массив исходных данных и результатов. На вход сети поступают исходные данные, а выход сравнивается с имеющимися данными. В зависимости от степени несоответствия полученной и контрольной выборок веса нейронов корректируются. Данный алгоритм обучения в основном применяется в задачах классификации, обобщения, распознавания образов и прогноза.

История альтернативной технологии

А сейчас небольшой экскурс в историю. Временем рождения нейрокомпьютинга считается 1943 год, когда вышла работа нейропсихолога Уоррена Маккалока (J. McCulloch) и математика Уолтера Питтса (W. Pitts) "Логическое исчисление идей, относящихся к нервной деятельности". В ней были сформулированы основные принципы построения искусственных нейронов и нейронных сетей. Потом психологами были созданы модели человеческого обучения. Естественно, что пытливые умы ученых попробовали их применить к нейронным сетям. Получилось.
В 1958 году Френк Розенблатт разработал модель перцептрона (от perception - восприятие). Его обучение требовало около получаса машинного времени на одной из самых мощных в то время ЭВМ IBM-704. Аппаратный вариант - Mark 1 Perceptron - был построен в 1960 году и предназначался для распознавания зрительных образов.
Первые успехи в области нейрокомпьютинга привлекли большое внимание научных и околонаучных кругов общественности, стало модным предсказывать скорейшее развитие искусственного интеллекта, создания искусственного разума и т.п.
Конец этому буму положил бывший однокашник Розенблатта по Высшей научной школе в Бронксе Марвин Минский, который в 1969 году выпустил книгу "Перцептроны". В ней он математически строго доказал, что нейронным сетям доступен лишь очень узкий круг задач. Несмотря на то, что его критика относилась к простейшей сети - однослойному перцептрону, массовые исследования и разработки были свернуты вплоть до 80-х годов прошлого века.
В 1982 году физик Джон Хопфилд с помощью новейших методов теоретической физики разработал модель ассоциативной памяти нейронной сети. Это пробудило интерес широкой научной общественности к некогда позабытым разработкам.
Исследования в этом направлении были возобновлены в 1983 году, когда развитие таких технологий стало финансировать Агентство перспективных военных исследований США (DARPA). Но широкое практическое применение нейросетей началось лишь после публикации в 1986 году Дэвидом Румельхатом метода обучения многослойного перцептрона, названного им методом обратного распространения ошибки (error back-propagation). Ограничения перцептронов, о которых писал Минский, оказались преодолимыми, а возможности вычислительной техники - достаточными для решения широкого круга прикладных задач.

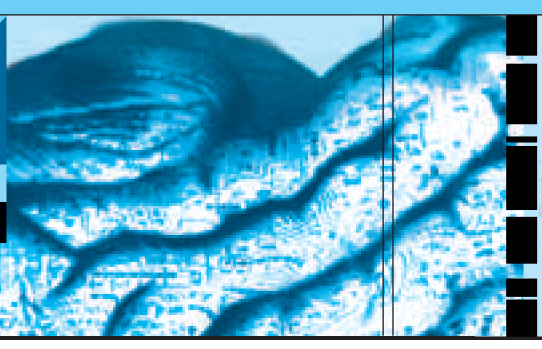
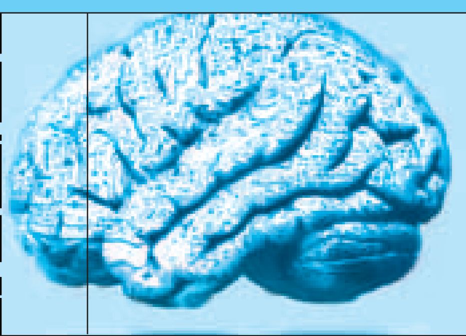
По заявлению Билла Гейтса, его корпорация собирается в ближайшее время выпустить новую операционную систему, 90% ресурсов которой будет занято распознаванием образов. А по признанию одного из топ-менеджеров Intel Роберта Экельмана, лидер рынка микропроцессоров серьезно готовится к новому технологическому витку, в частности, проводит дорогостоящие исследования в области биочипов, которые должны заменить в нейрокомпьютерах будущего обычные "железные" процессоры.

А что же сейчас?

А сейчас нейросетевые алгоритмы и нейрокомпьютеры в целом применяются во многих областях. Типичные задачи, которые решаются с помощью нейронной сети, обладают рядом характеристик:
- отсутствует алгоритм или неизвестны принципы решения задач, но накоплено достаточное число примеров;
- проблема характеризуется большими объемами входной информации;
- данные неполны или избыточны, зашумлены, частично противоречивы.
Именно поэтому нейронные сети хорошо подходят для распознавания образов и решения задач классификации, обобщения, оптимизации и прогнозирования.
Программное и аппаратное обеспечение на базе нейросетей уникально для решения каждой задачи. Основными заказчиками продуктов этой категории являются крупные финансовые корпорации, банки, спецслужбы, и т.п. Естественно, информация о применяемых технологиях не распространяется. Тем не менее, область применения нейрокомпьютеров весьма широка:
Так, для банков, страховых компаний это автоматическое считывание чеков и финансовых документов, проверка достоверности подписей, оценка риска для займов, прогнозирование изменений экономических показателей, автоматическое считывание документов.
В нефтяной и химической промышленности - анализ геологической информации, идентификация неисправностей оборудования, разведка залежей минералов по данным аэрофотосъемок, управление различными процессами.
Военная промышленность и аэронавтика применяют нейронные сети для обработки звуковых и инфракрасных сигналов, идентификации и интерпретации целей, обобщении информации, а также при автоматическом пилотировании.
В промышленном производстве управляют робототехникой и различными манипуляторами, применяют системы обнаружения неисправностей.

NEXT

Implant

КОМПЬЮТЕР БУДУЩЕГО

Елманов Олег (SpyDr@comail.ru)

Давно известен факт "встречной направленности" биологической и компьютерной эволюций. Человек сначала учится распознавать зрительные образы и двигаться, затем говорить, считать, и, наконец, самое сложное - приобретает способность логически мыслить абстрактными категориями. Компьютеры же, наоборот, сначала освоили логику и счет, потом научились играть в игры и лишь с большим трудом подходят к проблемам распознавания речи, обработки сенсорных образов и ориентации в пространстве.

В спецслужбах нейронные сети занимаются распознаванием лиц, голосов, отпечатков пальцев.
В телевидении и связи тоже применяются нейронные сети. Они занимаются такими задачами, как адаптивное управление сетью связи, сжатие, обработка сигналов и изображений.
Разумеется, это далеко не все. Нейрокомпьютеры находят все больше областей применения. Так, фирма LIAC выпускает аппаратуру для контроля качества воды. Нейросистемы фирмы SAIC находят пластиковые бомбы в багаже авиапассажиров. Специалисты инвестиционного банка Citicomp (Лондон) с помощью программного нейропакета делают краткосрочные прогнозы колебаний курсов валют.

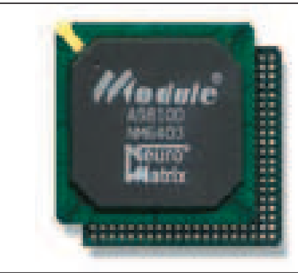
Процессоры с приставкой нейро

После почти тридцатилетнего затишья одной из первых возможностями нейронных сетей заинтересовалась компания Intel. Работы по этой теме были начаты в 1988 году. В следующем году уже был представлен первый рабочий образец нейропроцессора i80170NX ETANN (Electrically Trainable Analog Neural Network). Высокопараллельная архитектура, свойственная нейронным сетям, и ряд особенностей построения процессора позволили добиться быстродействия 2 млрд. операций в секунду. Следующим продуктом Intel стал цифровой нейропроцессор i80160NC, выпущенный в 1993 году.
Нейрочипы широко используются при решении перспективных военно-прикладных задач. Например, в США нейрочипы применяются в системах наведения высокоточного оружия, в высокопроизводительных комплексах криптоанализа, в системе по обнаружению пластиковой взрывчатки в багаже авиапассажиров, автоматизированных системах аутентификации личности по отпечаткам пальцев и другим антропологическим характеристикам человека.

Наш ответ империализму!

В 1998 году на мировой рынок нейрочипов вышел НТЦ "Модуль" с нейронным процессором NM6403. Разработанный российскими инженерами, нейропроцессор выпускается фабриками Samsung и позволяет решать ряд уникальных задач.

НТЦ "Модуль" продает нейропроцессоры NM6403. Стоят они не так уж дорого - около $50. Также выпускается ряд нейроплат на его базе (в формате PCI, CompactPCI и VME) с драйверами под Windows и Linux. Вся продукция обеспечивается специализированным софтом и поддержкой.



Нейропроцессор NM6403 производства НТЦ "Модуль"

Нейропроцессор обладает следующими характеристиками. Тактовая частота - 40 МГц; напряжение питания - от 3,0 до 3,6 В; потребляемая мощность - 1,3 Вт. Основные вычислительные узлы процессора - управляющее RISC-ядро и векторный сопроцессор. Производительность нейропроцессора составляет 120 млн. операций в секунду для 32-битовых операнд. Более полное описание и документация по нему представлена на сайте производителя - http://www.module.ru.
Детищем НТЦ "Модуль" заинтересовались крупнейшие мировые производители в сфере информационных технологий и связи. Так, европейское отделение Fujitsu планирует применять архитектуру для средств связи, требующих передачи и обработки видеоданных в реальном времени. Нейрочип показал себя высокопроизводительным процессором широкого применения для встраиваемых систем. Особенно он хорош для обработки видеоданных, радиолокации и криптографии. Примером может служить интеллектуальный детектор транспорта "Трафик-монитор", предназначенный для измерения в реальном времени статистических характеристик транспортного потока. Он позволяет измерить общее количество прошедших транспортных средств по каждой полосе движения, классифицировать транспортные средства по типам (мотоцикл, автомобиль, автобус и др.), расстояние между автотранспортом для каждой полосы и т.д.

А как насчет ПО?

Программное обеспечение для работы с нейронными сетями довольно обширно представлено на рынке. Можно найти все - от бесплатных небольших программок, работающих из командной строки, до промышленных нейросетевых комплексов масштаба предприятия.
Условно бесплатные и бесплатные продукты, как правило, разрабатываются студентами, аспирантами или энтузиастами. В основном они предназначены и оптимизированы для решения одной определенной задачи и имеют весьма примитивный интерфейс.
Следующий класс программного обеспечения составляют профессиональные продукты для моделирования нейронных сетей на персоналках. Вообще-то, нейронные сети только при обучении охочи до вычислительных ресурсов, а, будучи обученными, работают весьма шустро. Тем не менее, существуют продукты, поддерживающие аппаратные нейроускорители. Программное обеспечение данной категории, как правило, помимо расширенных возможностей работы с нейросетями, отличается подробной документацией, а также мощным графическим сопровождением работы. При этом они имеют один существенный недостаток - заоблачная цена.
Другой отряд нейросетевого ПО ориентирован на решение задач корпоративного уровня и оптимизирован под выполнение конкретных задач. Например, прогнозирование рыночных показателей, анализ степени благонадежности клиента и др.
Отдельную строку занимает промышленное нейросетевое ПО, эксклюзивное по сути и назначению, разработанное под конкретные задачу и "железо".

С 1995 года в России ежегодно проводится конференция "Нейрокомпьютеры и их применение". На ней представляются новейшие разработки в области нейротехнологий. Принять участие пока что могут все желающие, оформившие заявки в оргкомитете. С 1999 года издается журнал "Нейрокомпьютеры: разработка, применение". Журнал содержит статьи по вопросам разработки и применения современных нейрокомпьютеров.

Сделай сам!

Для того чтобы смоделировать нейронную сеть и решить с ее помощью какую-нибудь задачу (да хоть поиска той самой цыпочки), не обязательно учиться в МГУ или работать в одном из НИИ. Тебе надо будет установить один из пакетов для моделирования нейросетей. Обычно в них рассмотрены примеры и дана теория, достаточная для успешной работы. А вот и сами программы моделирования нейросетей.

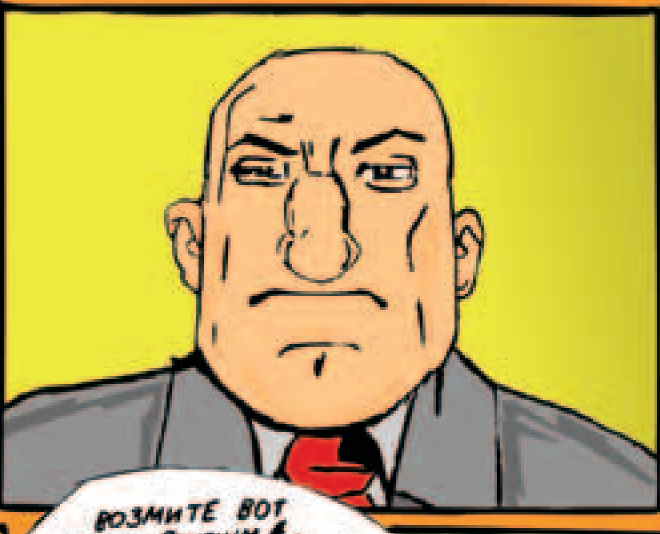
NeuralWorks Pro II/Plus

Один из мощнейших пакетов. Поддерживает ряд платформ (Intel, Sun Sparc, Silicon Graphics, IBM RS6000) и операционных систем (Windows, Linux, Solaris, Irix, AIX). Включает все известные типы нейросетей и алгоритмов обучения. Графически отображаются функционирование сети и средства диагностики. Стоимость в зависимости от ОС и платформы $1995 - $4995. Профессиональный вариант к тому же включает средства разработки, позволяя использовать и генерировать исходный код на Си, проектировать и разрабатывать новые нейросети. К тому же прилагаются специализированные пакеты для применения НС в реальном времени в совокупности с нечеткой логикой и генетическими алгоритмами. Такая "конфетка" и стоит соответственно: от 9995$ до 14995$. Последняя версия продукта 5.5.

NeuroSolution

Пакет довольно неплохой. Включает большинство широко используемых нейросетей и алгоритмов обучения. Программа проста в освоении, красивый графический интерфейс и хорошая система подсказок и помощи весьма кстати. Красочность картинок и инструментарий, позволяющий строить сети мышкой, создают ощущение игры. К тому же, программа хорошо работает по своему прямому назначению - есть программные ускорители и много других примочек. На сайте производителя выложена ознакомительная версия (12 Мб).
В целом, NeuroSolution можно порекомендовать для













автор story VIRUS



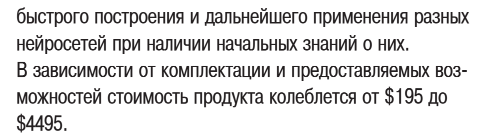
Новая история в следующем номере

подробности на
microlab-speaker.ru

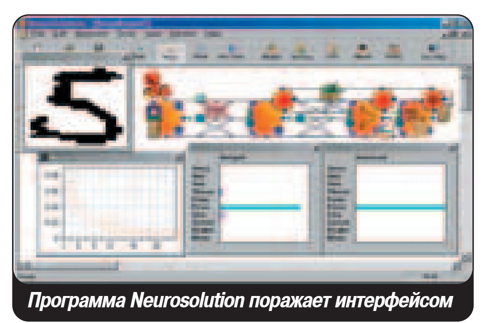
Implant

КОМПЬЮТЕР БУДУЩЕГО

Елманов Олег (SpyDr@comail.ru)



быстрого построения и дальнейшего применения разных нейросетей при наличии начальных знаний о них.
В зависимости от комплектации и предоставляемых возможностей стоимость продукта колеблется от $195 до $4495.

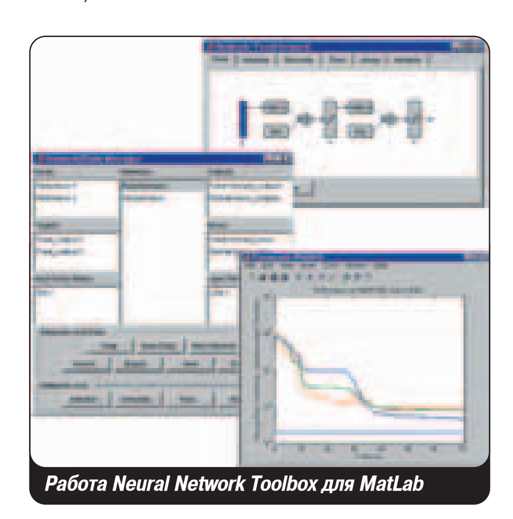


Программа Neurosolution поражает интерфейсом

Neural Network Toolbox для MatLab

Преимуществом продукта является популярность MatLab. Многие с ним сталкивались и имеют кое-какие навыки работы. В настоящее время распространяется четвертая версия Neural Network Toolbox. Она отличается улучшенным интерфейсом, а также джентльменским набором нейронных сетей и алгоритмов обучения. На возможностях, прелестях и недостатках MatLab останавливаться не буду, думаю, они известны. Добавлю, что Neural Network Toolbox произведена в лучших традициях родителя - много опций, различных примочек, прекрасная масштабируемость, правда, при этом MatLab поглощает все системные ресурсы. Цены на пакет, конечно, кусаются - сам MatLab стоит около $3000 плюс Neural Network Toolbox около $2000, что, в виду широкой популярности пакета, не останавливает Российского пользователя!

Уже через одиннадцать месяцев окупились инвестиции компании Autonomy, которая решила сделать ставку на разработку так называемого сетевого агента. Этот нейросетевой продукт представляет собой индивидуального электронного секретаря, который, изучив привычки и интересы хозяина, может успешно заменять его при работе в интернете.

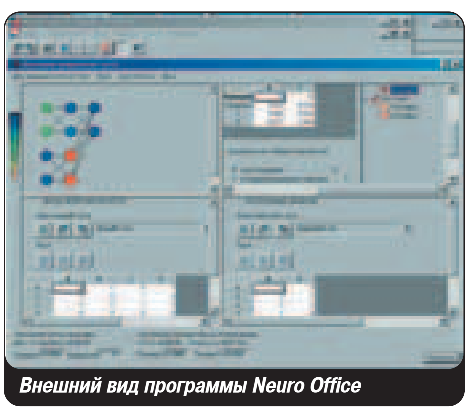


Работа Neural Network Toolbox для MatLab

Трехмерный график результатов обучения нейронной сети в MatLab

Neuro Office

Под столь громким названием скрывается разработка фирмы из Санкт-Петербурга "Альфа Систем". В программе доступны наиболее популярные типы нейросетей. Реализован программный интерфейс модели многокомпонентных объектов (COM-технология), что позволяет легко встраивать результаты проектирования в любое приложение Microsoft Office. Применять продукт разработчики предлагают в задачах прогнозирования, для построения экспертных систем, распознавания образов, цифровой обработки сигналов.
Пользовательский интерфейс нельзя назвать интуитивным. Один из недостатков - это то, что каждую связь между нейронами приходится задавать вручную. Не впечатляет и отсутствие диагностических сообщений о результатах работы, как на этапе конструирования, так и в процессе обучения и работы.
В целом, программа хорошо проявила себя при работе, хотя и страдает синдромом "искушенного разработчика": создателям и так все понятно, а вот пользователю со скромными знаниями придется помучиться. На сайте разработчиков предлагается демо-версия, полная же версия программы продается от $100 для образовательных учреждений России и СНГ и до $400 для иностранных пользователей.



Внешний вид программы Neuro Office

Не стоит думать, что другого ПО не существует. Существует, и очень много. Поищи, может, какой эксклюзив найдешь, поделишься! Количество программного обеспечения с применением нейросетей постоянно растет, и за всем угнаться просто невозможно. К сожалению, зарубежные нейросетевые пакеты слишком дороги, а отечественные разработки не могут в полной мере конкурировать на мировом рынке.

А как насчет девушки?
Нейросетевые технологии привлекают рядом уникальных характеристик:
- Параллелизм обработки информации - глобальность связей между нейронами. До обучения эти связи произвольны и малы. Обучение проявляет конкретную структуру сети под конкретную задачу.
- Надежность функционирования. Избыточность связей приводит к тому, что даже вывод из строя некоторого числа нейронов не сказывается критически на работе всей сети.
- Способность решать неформализованные задачи, которая следует из способности нейросетей самостоятельно вырабатывать весьма сложные алгоритмы обработки данных, формализовать которые порой не могут даже лучшие эксперты в этой области.

Кстати, задача определения самой клевой и красивой девушки еще не решена. Даже с использованием нейрокомпьютера. Может, у тебя получится? Дерзай!



Математический аппарат классических и самых распространенных видов нейросетей не так сложен. Программирование не требует профессиональных изощрений: на каждом шагу - умножение вектора на матрицу с накоплением суммы. Сложность представляет адаптация алгоритма обучения нейронной сети под конкретную задачу - подбор и моделирование сети, подготовка обучающего набора, предварительная обработка информации, анализ результатов.

http://www.neurok.ru - сайт российской инновационной компании "НейрОК".
http://webcenter.ru/~iprzhr/nejrcomp.html - журнал "Нейрокомпьютеры: разработка, применение".
http://neurnews.iu4.bmstu.ru/neurnews.html - новости с российского рынка нейрокомпьютеров.
http://www.module.ru - сайт НТЦ "Модуль".
http://user.cityline.ru/~alphasys/indexr.html - сайт питерской фирмы "Альфа систем".
http://www.mathworks.com - сайт компании MathWorks, производителя MatLab и Neural Network Toolbox.
http://www.neuralware.com - компания NeuralWare, производитель NeuralWorks Professional II/PLUS.
http://www.neurosolutions.com - здесь можно скачать пробную версию программы NeuroSolutions компании NeuroDimension Inc.
http://www.neuroproject.ru - компания "Нейропроект", производит нейросетевое ПО.



ВЫБЕРИ СВОЮ СКОРОСТЬ

Скорость от 128 Кбит/с до 7500 Кбит/с
в зависимости от тарифного плана.



ЖИЗНЬ ПОСЛЕ ЖИЗНИ

Abra http://mag.cyberpunk.ru

Жизнь после жизни

Даже после смерти можно жить

Смерть — понятие растяжимое

В разные времена люди принимали за смерть разные явления. Самые древние наши предки под смертью понимали прекращение дыхания, т.к. синонимами были слова «душа» и «дух». Врачи (или лекари) констатировали факт смерти, поднося к губам металлическое зеркальце. Если оно не запотевало – это означало отсутствие дыхания, а соответственно отлет души в мир иной. Чуть позже люди начали немного разбираться в анатомии и констатировали факт смерти уже с прекращением сердцебиения. В то время врачи начали замечать, что в некоторых случаях «труп» продолжал жить даже после прекращения дыхания. Нередко при вскрытии умершего оказывалось, что его сердце все еще продолжает биться. Поэтому запись в свидетельстве о смерти «вскрытие показало, что пациент умер в результате вскрытия» не раз имела место быть. К середине 20 века было введено понятие «клинической смерти», когда оказалось, что и после остановки сердца пациента все еще можно вернуть к жизни. Широкое распространение получили прямой и непрямой массаж сердца, а также электродефибрилляция – массаж сердца с помощью тока. Однако если в течение 20 минут пациента не удается вернуть к жизни, попытки, как правило, прекращаются - считается, что за это время в мозгу наступают необратимые изменения.

Криостаз не является широко распространенной процедурой лишь потому, что большинство людей просто не желает жить слишком долго.

Но тут врачи стали замечать, что пациенты, утонувшие в холодной воде, могут быть возвращены к жизни даже после истечения критического срока пребывания без дыхания, без сердцебиения и без функционирования головного мозга. Оказалось, что резкое охлаждение предотвращает повреждение мозгов. Такие случаи и положили начало теории криогенных технологий. Сейчас это уже не просто идея, ученые давно перешли от теории к практике, а в США полно фирм, предлагающих свои услуги по замораживанию как умерших, так и еще живых людей.

Суть крионики заключается в том, что любой организм можно заморозить, а по прошествии некоторого времени вернуть к жизни. Причем необязательно это проделывать именно с живым организмом. Если тело умершего человека не дошло до стадии разложения, его также можно заморозить, с надеждой в будущем разморозить и вылечить. В настоящее время подобным экспериментам подвергают себя безнадежно больные люди, например, зараженные СПИДом. Пока что лекарства от этой болезни не существует, а крионизация тела дает хоть какой-то шанс, пускай и маленький. Согласись, для безнадежно больных это наилучший вариант развития событий, против того, что у них есть сейчас. Правда, позволить себе подобную процедуру заморозки могут не все люди, т.к. число криостатов ограничено, а сама эта услуга довольно дорогая и по карману только обеспеченным людям.

После смерти Ленина один из ученых предложил заморозить вождя, чтобы в дальнейшем его разморозить и оживить. Для этого даже купили низкотемпературную холодильную установку из Германии, но в итоге все закончилось обычным бальзамированием.

Сам процесс

Процедура замораживания состоит из следующих этапов: 1) сначала кровь пациента заменяется кровезаменителем, устойчивым к низким температурам; затем производится насыщение тканей «трупа» раствором, который уменьшает повреждения при глубоком замораживании; 2) после начинается медленное охлаждение пациента, для этого его тело погружают в сухой лед; 3) теперь его перемещают в криостат, такой большой металлический термос, наполненный жидким азотом, и хранят там тело при -196 градусах по Цельсию. При такой температуре тело способно храниться в течение долгих столетий, нужно только раз в месяц пополнять запасы жидкого азота и раз в десятилетие производить ремонт криостата.

Криостат

Кстати, многие представляют себе криостат как одиночную камеру-капсулу. В принципе, это не удивительно, т.к. во всех фильмах это показано именно так. На самом же деле криостат рассчитан не на одного человека, а сразу на нескольких - обычно на пятерых; максимальное число пользователей - пятнадцать. Да и выглядит он несколько иначе: абсолютно герметичный непрозрачный куб, в котором располагаются сразу несколько тел, расположенных так, чтобы не мешать друг другу. В случае разгерметизации сосуда, придуманная технология резервуара позволит максимально быстро устранить последствия аварии, не нанеся никакого ущерба содержимому. Что же чувствует человек, находящийся внутри такого гроба? Ничего. Никаких эмоций, никакой боли, никаких ощущений или воспоминаний, абсолютно ничего. Для некоторых будет открытием узнать, что даже снов пациент не видит. Как известно, сны – это результат деятельности работы головного мозга, а замороженные клетки ни на какую деятельность не способны.

Информационная смерть

Рассмотрим подробнее, что происходит с мозгом, когда тело подвергается крионизации:

1) в течение нескольких секунд сознание гаснет. Внешние признаки жизнедеятельности исчезают, мышцы начинают обмякать;

2) уровень активности мозга падает до уровня, соответствующего состоянию сна. Начинаются сновидения, и если в этот момент пациента разбудить, у него останутся некоторые воспоминания. Обычно воспоминания связаны с ярким светом где-то сверху, с полетом («летаешь – значит, растешь!») и т.д.;

NEXT



Только что замороженное тело помещают в криостат



Implant

ЖИЗНЬ ПОСЛЕ ЖИЗНИ

Abra http://mag.cyberpunk.ru



Криостаты в лаборатории «Alcor»

3) примерно через минуту активность мозга падает до нуля. Нейроны мозга переключаются в состояние анаэробного метаболизма. Однако если кровоснабжение восстановить, они могут вновь вернуться к обычной кислородной жизни и восстановят нормальную электрическую активность;
4) после следующего этапа в мозгу наступают необратимые изменения. Это значит, что даже если восстановить кровоснабжение, работа мозга восстановится не полностью. Но важно знать, что это происходит не в результате гибели нейронов, а в результате того, что кровь в сосудах мозга сворачивается;
5) даже после окончательного прекращения функционирования нейронов, структура их связей некоторое время сохраняется. Это означает, что сохраняется теоретическая возможность восстановить нейронную сеть, идентичную исходной. По современным представлениям, именно структура связей между нейронами несет в себе «личность» человека;
6) наконец, в процессе разложения тканей структура связей между нейронами окончательно разрушается. Именно это сторонники крионики называют информационной смертью. До ее наступления сохраняется теоретическая возможность восстановления человеческой личности, после - такая возможность исчезает.
Экспериментально установлено, что после замораживания нейронов млекопитающих до температуры жидкого азота и последующего размораживания, их жизнедеятельность восстанавливается; восстанавливается также электрическая активность в образцах нервной ткани. Структура связей между нейронами может сохраняться в течение сотен лет.

Текущее положение дел

Загвоздка крионики в том, что современная наука не знает способа разморозить человека без нанесения вреда его мозгу и телу. Технология оживления совершенно иная, чем первая стадия крионизации. В настоящее время люди научились осуществлять полный цикл замораживания-размораживания только объектов небольших размеров, таких как яйцеклетки, эмбрионы, фрагменты кожи и т.п. Были случаи успешного оживления маленьких животных, но даже это пока что не позволяет осуществить полный цикл крионизации человека.
Несмотря на такое положение дел, в настоящее время официально признаны замороженными более 100 человек, а еще около 1000 подали заявки и готовы стать полуфабрикатами хоть завтра. И все это за довольно высокую цену на услугу, гарантия на выполнение которой не предоставляется. В США наблюдается настоящий бум среди компаний, предоставляющих услуги крионизации, такие компании растут и пухнут с каждым годом. Стоимость процедуры заморозки стоит по-разному: от 150 до 300 тысяч баксов. Некоторые фирмы предоставляют даже шанс оплатить свои услуги в рассрочку. В действительности же заморожено уже намного больше людей, чем это известно официально. Дело в том, что все фирмы имеют дополнительную услугу о «неразглашении договора», проще говоря, за небольшую плату они перестают трепать языком. Так, например, до сих пор неизвестно, удовлетворили ли желания Сальвадора Дали и Уолта Диснея заморозить их тела. Самой известной замороженной личностью на сегодня (о которой известно обществу) можно считать американского актера и продюсера Дика Джонса.

На первый взгляд может показаться странным желание пациентов или их родственников заморозить труп. На самом деле ничего странно здесь нет, даже наоборот. С развитием медицины количество времени, в течение которого есть возможность реанимировать человека, стало расти, и если 50 лет назад это было 6-8 минут, то теперь уже около 20. В отдельных же случаях реанимировать человека после остановки сердца или дыхания удавалось и через больший промежуток времени. Поэтому когда сегодня замораживают людей после клинической смерти, шансы на их оживление в будущем чрезвычайно высоки. Но из-за юридических проблем тело сегодня можно заморозить только в случае, когда врач признал смерть пациента, т.е. по прошествии нескольких часов после остановки сердца или дыхания, что неблагоприятно сказывается на состоянии тела.

Оживление

Для оживления тела ученые хотят использовать принцип нанотехнологии. Одним из устройств, разрабатываемых в рамках нанотехнологии, являются молекулярные роботы - роботы размером с молекулу. Такие машинки будут снабжены миниатюрными вычислительными устройствами и манипуляторами, позволяющими работать с молекулами, например, перемещать их и модифицировать структуру, т.е. заниматься молекулярной хирургией.
Возможный сценарий оживления выглядит следующим образом:
1) в замороженное тело внедряется огромное количество (миллионы миллиардов) молекулярных роботов, чей совокупный вес составит около 500 г;
2) они анализируют повреждения, возникшие в клетках организма в результате его смерти. При необходимости они обмениваются информацией между собой и контролирующим их деятельность компьютером, который располагается вне тела;
3) на основе этого анализа они производят исправление всех этих повреждений. Кроме этого они производят омолаживание и лечение клеток (а значит и всего организма) - т.е. оживлен будет не старый и больной организм, а здоровый и омоложенный;
4) после выполнения задания молекулярные роботы покидают оживленное тело, например, через кровеносную систему и дыхательные пути.

По современным оценкам подобная процедура может занять несколько месяцев. Технология для ее реализации будет готова через 50-100 лет. Т.е. крионизированное тело должно сохраняться в течение этого промежутка времени. А это, как известно, не проблема.

> Сейчас только в США существует как минимум 6 легальных компаний, предлагающих услуги крионизации.

Напоследок

По результатам исследований, которые проводили американские социологические компании, стало ясно, что основным препятствием для развития криогенных технологий в России являются не столько финансовые проблемы, сколько нежелание самих людей жить дольше. Россияне примирились с мыслью о неизбежности смерти и в действительности, а не на словах, не хотят жить дольше обычного, да еще и платить за крионизацию своих тел.

Ссылки по теме:

Alcor Life Extension Foundation
www.alcor.org
Cryonics Institute
www.cryonics.org
Kryos Biomedical
www.kryosbiomedical.com
American Cryonics Society
www.jps.net/cryonics
European Cryonics Support Group
www.cryonics-europe.org
Новости крионики
http://cryonews.euro.ru

mindw0rk

][NEWS

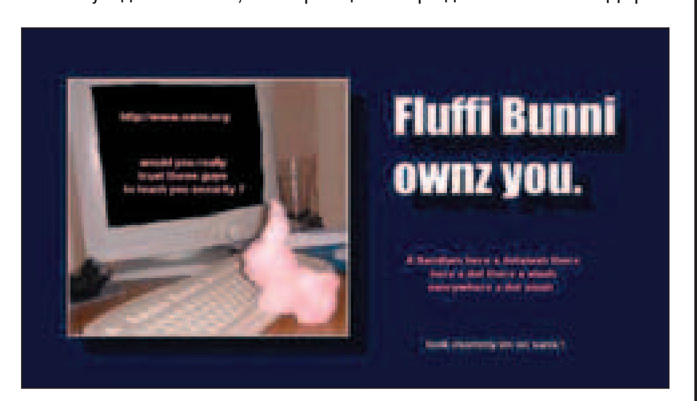
СПАМЕРСКИЙ РЕЙД RIAA

"Слющай да, выследить тебя, засранца, нам раз плюнуть и мы не фиг делать можем привлечь тебя к суду и страшной ответственности. Поэтому, если не хочешь сидеть на нарах до конца жизни - перестань, говнюк ты эдакий, юзать пиринговые сети и давать скачать корешам своей музон", - сообщения примерно такого содержания получили по аське более миллиона пользователей napster-подобных систем. Воистину спам - универсальное оружие для решения самых разных задач. Для RIAA он стал оружием возмездия против всех халявщиков, мешающих крупнейшей звукозаписывающей компании грести бабки лопатой. "Вы занимаетесь воровством! Вы нарушаете закон! Сверните с этого пути пока не поздно", - то ли просит, то ли угрожает РИА. Не знаю, насколько в США считается преступление дать переписать приятелю музыку со своего винта, но то, что спам там вне закона - это точно. Так что, если компания будет продолжать в том же духе, вполне возможно, юзеры Grokster, Kazaa и других пирингов соберутся все вместе и сами подадут на спамера в суд. Не рой другому яму, РИА!



FBI OWNZ YOU, FLUFFI BUNNI

ФБР, наконец-то, арестовала одного из самых известных дефейсеров мира - хакера Линн Хтунга aka Fluffi Bunni. Кто не знает - этот чел последние три года только и делал, что взламывал сайты известных организаций и на место стартовых страничек вставлял картинку розового плюшевого кролика с подписью: "Fluffi Bunni ownz you" (тебя поимел плюшевый кролик). Большую любовь Линн питал к security-компаниям и пагам, посвященным сетевой безопасности, которые прилюдно высмеивал. Несмотря на сомнительную деятельность, квалификация хакера довольно высока. Дефейсами Линн занимался в качестве хобби, остальное время уделяя работе в сфере security. Но осторожность и знания кролику не помогли. Приехав на лондонскую конференцию для специалистов по компьютерной безопасности InfoSecurity Europe 2003, Линн Хтунг с удивлением обнаружил, что там его уже ждут. "FBI ownz you, Fluffi Bunni" - с чувством произнес сотрудник спецслужб и надел на хакера наручники. Сейчас парень ожидает приговора, который, судя по всему, будет не самым приятным.



ЦЕНТРУ РАЗГОВОРНОГО АНГЛИЙСКОГО ТРЕБУЕТСЯ

Изрядно повеселило вашего покорного объявление, недавно появившееся на job.ru:
"11:14:45 | Должность: системный администратор, Город: Москва, Пол: Не имеет значения, Образование: Не имеет значения, Опыт работы: 3 года, Занятость: Любая. ЦЕНТРУ РАЗГОВОРНОГО АНГЛИЙСКОГО требуется системный администратор с опытом работы по отражению хакерских атак из интернета. Контактное лицо: American Language Center Телефон: 238-33-86 / 778-9894 / 411-0232". Возможно, это просто чья-то шутка, но хочется верить, что главного спамера рунета действительно удалось настолько достать, что он пошел на подобные меры. Будем надеяться, что скоро на том же сайте появится объявление от Центра о поиске врача, лечащего переломы.

УКРАИНА ВПЕРЕДИ ПЛАНЕТЫ ВСЕЙ

Американское правительство подвело итоги исследования в сфере пиратской индустрии и обнародовало рейтинг самых пиратских стран. В который раз испытываю гордость за свою страну - Украина возглавила список из 50 держав! В ходе исследования оценивалась доля пиратской продукции на рынке, размер ущерба от деятельности местных пиратов и меры борьбы с ними. Украина сделала всех. И действительно, я уже не помню, как выглядит лицензионный диск, и даже не представляю, где его у нас можно купить. Из-за полного пофигизма к авторскому праву, вильна краина попала в Priority Foreign Country - список самых злостных нарушителей международных правил торговли. Но Кучме это, очевидно, до лампочки, поэтому американцы сами срочно ищут решение, которое покончит с пиратством на Украине раз и навсегда (какие наивные). Следом за хохляндией в рейтинге идут Россия, Бразилия, Польша и Тайвань.

КАК ВЗЛОМАТЬ XBOX?

Автор нашумевшего взлома Xbox - Эндрю Хуанг aka Bunnie - недавно закончил работу над книгой о том, как захакать до смерти поделку от Microsoft. В "Hacking the Xbox: an Introduction to Reverse Engineering" несколько глав, в которых описываются устройство и работа мод-чипов (на них базируется приставка), лазейки для осуществления взлома, технология перехвата шифровального ключа и много других технических премудростей. Помимо чисто хакерских советов, Эндрю включил несколько рекомендаций сотрудникам Microsoft по улучшению защиты своего продукта. Основная проблема, с которой столкнулся автор - боязнь издателей публиковать руководство такого рода. Хотя тема освещается с разных сторон, при желании Эндрю можно обвинить в нарушении DMCA, а книгу запретить. Но Bunnie не отчаивается, и решил пока распространять "Hacking the Xbox" своими силами. На личные средства он отпечатал тысячу экземпляров и продает их сейчас через интернет на сайте http://hackingthexbox.com.



ДЫРЯВЫЙ ПАСПОРТ MICROSOFT

Пару месяцев назад группе неизвестных хакеров удалось обойти систему защиты Microsoft Passport - службы хранения конфиденциальной информации, которой пользуются двести миллионов человек. Непонятно как, но взломщикам удалось получить пароли к 200 аккаунтам. С ними они могли вытворять все что угодно. Когда инфа всплыла, похаканные "бумажники" были заблокированы. Но оставался вопрос - как это произошло? Ответ на него дал пакистанский независимый компьютерный эксперт Фейзал Данка Мухаммед. Будучи пользователем пресловутой системы, он заинтересовался, каким образом ее, а заодно и его самого, поимели. Найденное Мухаммедычем решение оказалось простым до безобразия. Всего-то и нужно - определенным образом подменить обратный адрес и запросить в техсуппорте пароль. После того, как информация об этом появилась в сети, Microsoft в срочном порядке заделала дырку. Но несмотря на это, теперь ей грозит несколько миллиардов, а то и триллионов долларов взысканий. В 2002 г. корпорация, уверенная в непотопляемости своей системы, взяла на себя обязательство выплачивать 11 тысяч долларов за каждый взломанный бумажник. А тут риску подверглись все пользователи. Сколько Биллу Гейтсу придется отстегивать за свои амбиции, и придется ли вообще, будет решать суд.

МЕСТЬ ХАКЕРУ ПРИВЕЛА К ТРАГЕДИИ

Не знаю, чем насолил Бисванат Халдер молодому сотруднику университета Case Western Reserve Шону Миллеру, но чем-то насолил. Иначе не стал бы Шон взламывать хоумпагу Халдера и стирать всю инфу с сервака. Для Бисваната эта хоумпага была не просто хоумпагой, это было его любимое детище! Он над ней месяцами корпел, черт побери. А тут какой-то сосунок... Короче, Бисв решил наказать сукина сына и упрятать его лет на сто куда поглубже и потемнее. Но ни ректор универа, ни полиция, ни мэр, ни ФБР, ни президент Джордж Буш, которым адресовала свои жалобы жертва хака, не пошли навстречу и даже не посочувствовали Халди. "Ну вы, мля, заплатите!" - прошипел Бисв, достал дедово ружье и захватил CWR. 7 часов велись переговоры, во время которых в здании вуза находилась куча заложников. А когда полиция поняла, что лялякать тут бесполезно, началась резня. Террарюгу удалось подстрелить и арестовать, но перед этим он успел прикончить 30-летнего аспиранта Нормана Уоллеса. "Мне нужен был Миллер, всего лишь Миллер, понимаете?" Но никто его не понимал. И до сих пор не понимают. Даже сокамерники, которым теперь Халдер рассказывает свою грустную историю.

МАДОННА VS ХАКЕРЫ: КТО КОГО ПОИМЕЛ?

Как оказалось, у Мадонны неплохое чувство юмора. Наблюдая за безуспешными потугами RIAA противостоять пиратству, некогда-поп-королева поняла, что рассчитывать на эту контору бесполезно. Поэтому решила действовать по-своему. Как известно, недавно вышел ее новый альбом American Life. И, ясен пень, гадкие пираты захотят украсть ее песни, лишить тех денег, которые пойдут на



покупку домика в деревне. Но Мадонна проявила просто чудовищное благородство. Она выложила все песни из альбома на своем официальном сайте www.madonna.com для свободного скачивания! Офигевшие от такой щедрости поклонники навострили модемы и стали быстренько скачивать халявное добро. Ан не тут-то было. Слив и запустив новые сонги, вместо чувственного ритма, юзер слышал ехидный Мадоннин голос: "What the fuck do you think you're doing?" ("Ну че, поимела я тебя, жопа доверчивая?"). Но в то время как Мадонна со своим бойфрендом пили шампань и ржали над тем, как умело они развели своих фанатов, на чьем-то мониторе уже мигала фраза "Root been got. Fuck it down? Y/N". "Конечно да!" - воскликнул неведомый хакер и принялся разделывать сайт зарвавшейся звезды. Когда на следующий день Мадонна включила комп и зашла на свою страницу, то чуть копыта не отбросила - ее встретила надпись "This is what the fuck I think I'm doing" ("Это я тебя поимел, жопа старая") и весь драгоценный альбом с настоящими песнями в свободном доступе.

ДЛЯ ВЗЛОМА СМАРТКАРТ ДОСТАТОЧНО ЛАМПОЧКИ

Медленно, но верно на смену кредитным картам приходят смарткарты. На вид они ничем не отличаются, но внутри смарткарта содержит память и процессор. А в памяти можно хранить данные. Защита новых карточек очень сильна - на нее угрохали не один мешок денег, потратили черт знает сколько времени. Другими словами, взломать ее практически импоссибл. "Хрен вы угадали", - вдруг радостно воскликнул Судхакар Говиндавахайла, достал лампочку и хакнул карту в два счета. "А? Шо? Как?" - засыпали спецы вопросами студента из Принстона. "Элементарно, Ватсоны!" - ответил Судхакар. "Из-за лампового тепла у битов внутри чипа происходит солнечный удар, от этого они изменяют свое значение (с 0 на 1, с 1 на 0). Защита этого не выдерживает и ваша смарткарта становится не smart, а очень даже stupid". И, пошаманив лампочкой, студент продемонстрировал, как легко можно взломать и перепрограммировать кусок пластика.



Воистину, все гениальное - просто. Вот я теперь думаю, может мне взять пылесос и повозюкать им по ближайшему банкомату. Авось тамошние биты кондрашка хватит и меня засыплет баксами.



HACK-FAQ

О. Брун (hack-faq@real.xakep.ru)

Задавая вопросы, конкретизируй их. Давай больше данных о системе, описывай абсолютно все, что ты знаешь о ней. Это мне поможет ответить на твои вопросы и указать твои ошибки. И не стоит задавать вопросов вроде "Как сломать www-сервер?" или вообще просить у меня "халявного" Internet'а. Я все равно не дам, я жадный :)

<???> Ситуация такая: провайдер дает тестовый доступ на свою страничку. Как мне лазать по другим сайтам, например, xakep.ru?

A: Самое простое решение: добыть список ресурсов, доступных с сервера провайдера. Часто по тестовому логину можно увидеть все сайты, что размещены у прова. Если имеется хостинг приличных размеров, там можно отыскать интересные ресурсы. Метод насколько прост, настолько и неэффективен: бесплатный доступ, откуда был бы виден xakep.ru, хрен отыщешь :). Х будет не Х, если не предложит эффективного способа! Поставь CGI-прокси на сервер провайдера так, чтобы скрипт работал как обычный HTTP-прокс и позволял мутить соединения на веб. Метод не всегда работает, т.к. нужен рабочий логин на заливку и запуск скриптов. Также провайдеры часто закрывают доступ к серверу домашних страниц с гостевого входа. Еще рабочей остается тема туннелинга, т.е. передачи нужных нам пакетов по иному протоколу: заворачиваем HTTP в ICMP, пуляем пакет, получаем ответ - распаковываем посылку обратно в HTTP. Проблема решается софтом X-Proxy от deil'a - http://www1.xakep.ru/post/16337/default.asp. Существуют аналогичные проги, но большинство из них требуют установки серверной части: скрипта, который будет висеть где-то на сервере в инете, чтобы принимать и обрабатывать присланные ICMP'шки. Туннелить получится не только ICMP. Дополнительный материал можно увидеть на сайте underlings - http://huniver.org.ru/.

<???> Беру у барыг DVD, потом возвращаю. Хотелось бы копировать диски в DivX. Какой нужен софт?

A: Софта имеется масса. Разница лишь в том, что отдельные тулзы стягивают (рипают) фильм, а другие перегоняют стянутое в нужный формат; третьи же выполняют обе функции. Рассмотрим лишь третью опцию. Для краткости предложу DVD Master Backup. Прога бесплатная, последнюю версию можно стащить здесь: http://twtelecom.dl.sourceforge.net/sourceforge/dvdmb/.

<???> Как узнать, что стоит у чувака - прокси или его реальный (провайдерский) IP?

A: Универсальный способ - воспользоваться собственной логикой и WHOIS-сервисом (ripe.net, arin.net, etc.): ты знаешь, что чел живет в Бердичеве, почему же у него IP на Брайтон-Бич? Очевидно, что имеет место прокси. Если же просвечивается dial-up адрес, приписанный к местному прову, то чел - прозрачный и не пользуется "прокладками". Конечно, бывают сложности: чел живет в Америке (родной ИП на *.*.rr.com) и сидит под американским прокси (*.*.aol.com). Тогда на помощь придет простейший скан портов чувака: глянем на любимые прокси-порты: 80, 1080, 3128, 8080. Если порт отвечает, пробуем заюзать прокси. Получилось? Ясно, значит, клиент шифруется и ИП левый. Конечно, могут быть обломные исключения: прокс висит на нестандартном порте (часто сделанный обыкновенным порт-редиректом), трафик идет через VPN (Virtual Private Network) или все делается ssh-туннелингом.

<???> Какая связь между usenet и варезом? Как найти эту связь? ;)

A: Упомянутая связь была установлена еще до женитьбы вареза на www! С давних времен Usenet'ы были исправным источником вареза: там можно разыскать самый редкий варез, который будет разбит на десятки и сотни частей для наиболее удобной скачки. Стягивать варез обычным Outlook Express - долго и неудобно, существуют десятки прог серии newsgrabber (новостные грабли), заточенных под выкачивание графики, mp3, видео и вареза с news-серверов. К примеру, таким образом был успешно слит релиз Windows Server 2003. Искать варезку нужно по любимому ключику 'warez'. Самих существующих групп множество. К сожалению, большинство из них недоступно с бесплатных news-серверов, вроде news.fido7.ru. Да и на провайдерских часто урезают доступ к закачке вареза с usenet под ноль. Самый добротный доступ к варезке через новости наблюдался у американского ATT, когда тот успешно натягивался по dial-up в Москве. Мой нынешний пров, несмотря на официальную подписку на alt.warez, убеждает, что там нет ни одного постинга... Так что часто приходится разыскивать дополнительные news-машины. Из конкретного софта можно порекомендовать GrabIt! (www.shemes.com), который отлично высасывает эту варезку.

<???> Что такое палка? Чего с нее можно поиметь?

A: Берешь палку, отбираешь с ее помощью копейки у детей возле геймклуба :). На самом деле, это относится к кардингу. Палка - аккаунт в системе PP (PayPal www.paypal.com), дающий возможность оплаты по креде самых разных сервисов в сети: начиная с покупки вещей на аукционе и заканчивая посылкой денежных чеков по всему миру. Для обмана системы используется инфа по чужим кредиткам, которые приписываются к аккаунту. После создания аккаунта можно покупать вещи на сетевых аукционах, например, ebay.com. Живые деньги чаще всего циркулируют внутри США, т.е. чек из системы отправляется на имя "нальщика" (чела, обналичивающего деньги, пришедшие с палки), проживающего в Америке. Существует практика обмена или торговли "заряженными" аккаунтами, т.е. палками с уже прикрученной кредиткой для надоя. Наиболее ходовые места трейдинга (обмена/торговли) - IRC, каналы #cc #carding в крупных сетях. Ну вот, теперь ты не будешь краснеть, услышав: кинь мне палку, а может две...

<???> Правда, что сломали hotbox.ru? Как так получилось?

A: О "взломе" в прямом смысле слова, т.е. захвате сервера с последующим дефейсом, известно не было. Человек по имени error нашел весомую уязвимость в веб-интерфейсе почты, которая позволяет послать письмо юзеру, содержащее тег на зловредный скрипт. При хитром подходе открывается масса возможностей - от захвата ящика до массовой рассылки по спам-листу. Напомним, что Hotbox - лишь торговая марка, которая также скрывает в себе другие сервисы мыла, вроде mailru.com, pisem.net, rbcmail.ru. Так что несколько дней, пока дырка заделывалась, можно было натворить гадостей юзерам почтового портала. Подробнее читай здесь: http://www.void.ru/content/1074.

<???> Возле геймклуба пацаны у маленьких ребят отбирают деньги. Что делать, надо выправить нашу security?

A: Сбивайтесь в команды человек по 5-7: обычно гопники наезжают только на одиноких игроков. Но собираться в группы получается не всегда, тем более, если идешь играть в ночь, т.к. в это время люди любят спать. Можно завести какое-нибудь оружие самообороны, но проблема ограничения по возрасту (приобретение и ношение от 18 лет) остается. Если проблема не беспокоит, можно взять "Удар" - недорогой газовый "типа пистолет". Хорошо зарекомендовала себя в обороне "Оса", которая стреляет специальными патронами, оставляя нехилые следы на теле гопника. Работают и давно знакомые газовые баллоны, лучше, если с перцем ("Шок", "Скорпион"). Иногда придет на помощь электрошокер ("Кобра", "Гром"). Хотя, конечно, оружие - не самый умный выход, особенно при постоянном хождении в один клуб, т.к. гопники могут поймать тебя позже. Мы не особые сторонники совместной работы с чекистами, но в критической ситуации можно и "02" набрать, по крайней мере - предупредить о подобной возможности нападающих уродов. Конечно, трубку тоже могут отобрать... но лучше ее иметь при себе: мобилу можно новую купить, с покупкой здоровья сложнее. Стоит попробовать себя в боевых рукопашных делах, т.е. начать заниматься каратэ, дзюдо, самбо или боксом. Если даже и не будет возможности показать свои навыки гопам, сможешь продемонстрировать боевой дух. Будь в курсе последних средств самообороны, тактик защиты от уродов - читай конференции вроде "Самооборона в России" на www.guns.ru или "Криминал и защита" на www.auto.ru.

<???> Нахакал шелл доступ (ssh) к серверу, ftp нет. Как наиболее удобно слить оттуда нужное файло?

A: Если слить необходимо на удаленную машину - самым простым будет ftp, с, очевидно, предварительным man ftp ;). Если файлы нужно слить в мыло, все так же просто - mail, mailx... Скорее же всего тебе потребуется откачать инфу на локальную win-машину. Тогда удобнее воспользоваться SecureFX (www.vandyke.com), CuteFTP Pro (www.cuteftp.com) или впаять плугин в любимый файловый менеджер (у меня это SFTP для WinCmd - www.wincmd.ru/wfx_plugins.shtml).

<???> В WinXP не работает открывалка паролей для соединений с инетом, которую я юзал в Win98. Что делать?

A: В прошлом выпуске Hack-FAQ'а объяснялось, как вытягивать пароли из XP. Однако посыпались требования выдать готовое решение, эдакую программную хакалку. Самой маленькой и эффективной показалась Dialupass. 29K удовольствия берутся здесь: http://nirsoft.cjb.net.



TIPS&TRICKS

Если при старте The Bat! в командной строке (или в свойствах ярлыка) добавить /NOLOGO, при запуске не будет появляться сплеш-скрин (лого). Это позволит чуть-чуть уменьшить время загрузки. Если The Bat! запустить с параметром /CHECKALL, то The Bat! проверит почту всех незапароленных ящиков, после чего закроется. Открыв русифицированный TheBat.LNG hex-редактором, можно вместо стандартных надписей написать что-нибудь свое! А если ты забыл пароль, который ставил на аккаунт в The Bat!, то просто открой ACCOUNT.CFG, находящийся в соответствующей директории, hex-редактором и увидишь его там! :)

Garik
http://www.webhowto.ru/reg

Хочешь увидеть свои советы в журнале? Присылай их на адрес Sklyarov@real.xakep.ru. Ведущий рубрики Tips&Tricks Иван Скляров.

TIPS&TRICKS

Как известно, лицензионная Windows XP при переустановке системы требует повторной активации. Чтобы этого избежать, достаточно перед переустановкой системы скопировать файл wpa.dbl, расположенный в папке Windows\System32, например, на дискету - именно в этом файле хранится код активации. После переустановки системы, естественно, нужно будет заменить файл wpa.dbl на тот, что записан на дискете.

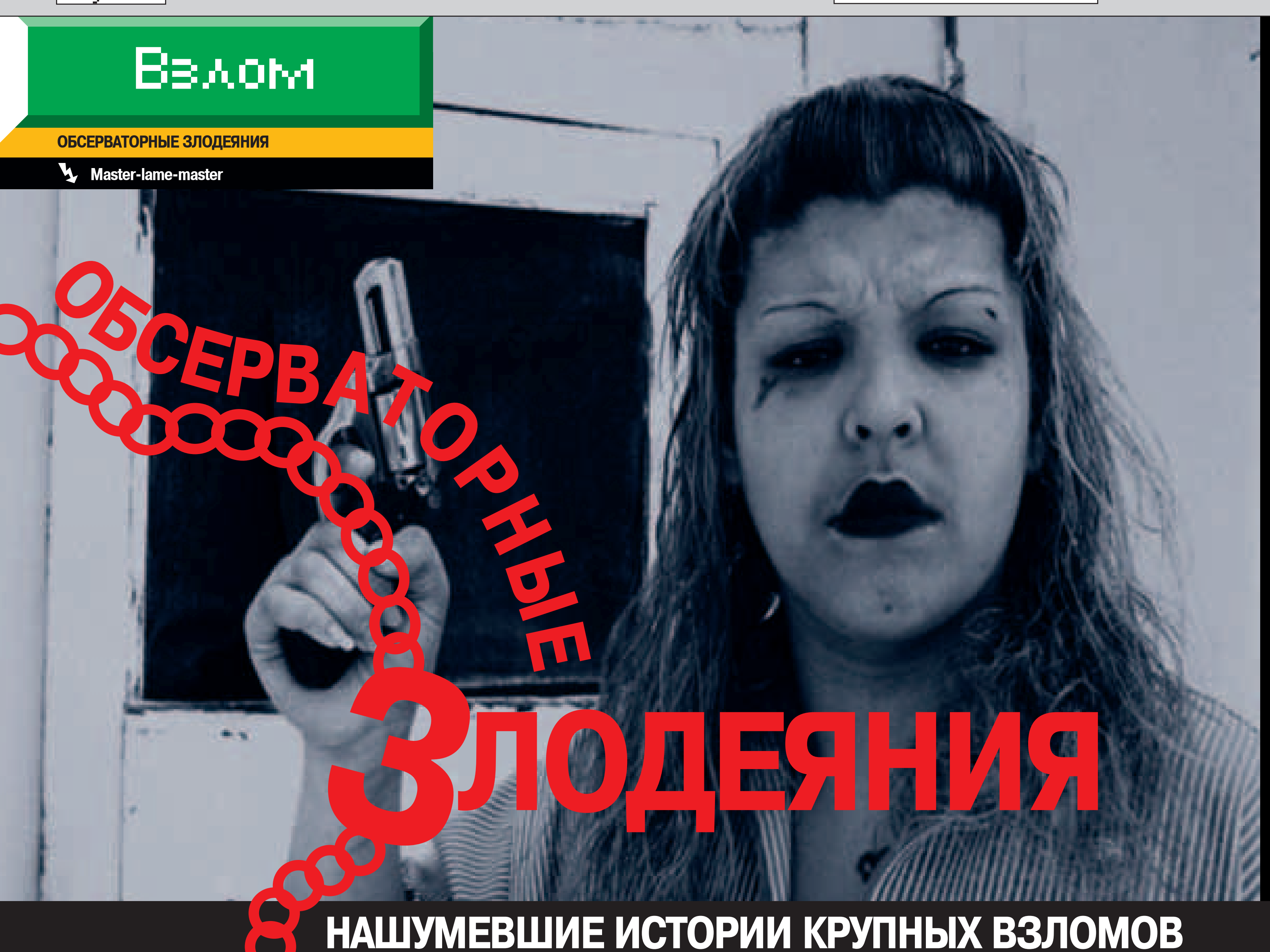
Garik
http://www.webhowto.ru/reg

Хочешь увидеть свои советы в журнале? Присылай их на адрес Sklyarov@real.xakep.ru. Ведущий рубрики Tips&Tricks Иван Скляров.

Взлом

ОБСЕРВАТОРНЫЕ ЗЛОДЕЯНИЯ

Master-lame-master



ОБСЕРВАТОРНЫЕ ЗЛОДЕЯНИЯ

НАШУМЕВШИЕ ИСТОРИИ КРУПНЫХ ВЗЛОМОВ

Тебе, наверное, не раз приходилось задумываться над вопросом: кто такие хакеры? Если верить словарю, то "хакер" дословно переводится как "крушитель".

На самом деле, этим скудным определением слово "хакер" не ограничивается. Всех хакеров можно разделить на несколько типов. Существуют разные классификации, но самая популярная включает лишь три категории:

1. Скрипткидди или начинающие хакеры. Ломают сервера через известные бреши в cgi/php скриптах. Как правило, дело ограничивается красивым дефейсом, наподобие "Hacked by 31337 h4x0r" :).
2. Хакеры-экстремалы. Для них взлом - праздник души. Используя public-эксплоиты, они вламываются в систему и делают с ней все, что захотят. Некоторые взломщики этого типа запросто могут разрушить операционку, которую только что взломали. К этой же категории относится, как ни странно, большинство хакеров, познавших азы взлома и маскировки в системе.
3. Профи. Наименее распространенный тип. К нему относятся настоящие гуру, занимающиеся сложным профессиональным взломом. Они работают на заказ и преследуют определенную цель, после достижения которой забывают о взломанном сервере.

ВЗЛОМ WWW.SAO.RU

Однажды экс-сотрудник московской астрофизической обсерватории предложил одному продажному хакеру очень заманчивое дельце. Как выяснилось из непродолжительной беседы, человека уволили с работы, а на его машине остались важные документы, которые должны быть уничтожены. Все бы ничего, но, по словам заказчика, эта машина являлась локальным сервером в крупной компании и видела сеть исключительно через NAT. Таким образом, чтобы проникнуть на сервер, хакеру пришлось бы взломать как минимум две машины, что сильно усложняло поставленную задачу. В завершение разговора заказчик сказал, что поверит в то, что работа выполнена, лишь в случае предоставления ему списка всех документов в папке /usr/biblio/docs (попросту говоря, после выполнения команды ls -la /usr/biblio/docs).

Недолго думая, взломщик зашел на web-сайт обсерватории, надеясь поискать баги в cgi/php скриптах, но тут же обломался. Весь сайт был сделан исключительно на html. Это заставило хакера призадуматься: то ли админы борются за безопасность такими радикальными мерами, то ли наоборот, не знают о существовании языков программирования для web. Взломщик понимал, что ломать через веб не имеет смысла. Поэтому пошел стандартным путем: залез на неприметный буржуйский шелл и просканил nmap'ом подсеть C, принадлежавшую обсерватории.
После часа безопасного stealth-сканирования хакер получил текстовый лог с информацией об открытых портах и операционках на серверах Sao. Практически все машины в сегменте были прикрыты фаерволом, только главный www-сервер оказался исключением, поэтому наш герой решил начать взлом именно с этой машины.

Таблица 1

```
Interesting ports on
relay.sao.ru (194.85.27.3):
(The 1554 ports scanned but not shown below
are in state: filtered)
Port      State    Service
21/tcp    open     ftp
22/tcp    open     ssh
25/tcp    open     smtp
80/tcp    open     http
110/tcp   open     pop-3
113/tcp   open     auth
10000/tcp open     snet-sensor-mgmt

Remote operating system guess: Linux 2.1.19
- 2.2.20
Uptime 9.120 days (since Fri Apr 11 17:16:07
2003)
```

Доверяя fingerprint'у сканера, хакер понял, что добить систему локально не составит труда (prtace баг еще никто не отменял). Вооружившись netcat'ом, нарушитель сетевого порядка пошел снимать баннеры с портов:

Таблица 2

```
[root@belgium root]# nc
194.85.27.3 21
220 relay.sao.ru FTP server (Version wu-2.6.1
(1) Wed Aug 9 05:54:50 MSK 2000) ready.
user ftp
331 Guest login ok, send your complete e-mail
address as password.
pass ftp
230-The response 'ftp' is not valid
230-Please use your e-mail address as your
password
230- for example: joe@belgium.shell.be or
joe@
230-[belgium.shell.be will be added if pass-
word ends with @]
230 User ftp logged in. Access restrictions
apply.
^C punt!
```

Н-да, встретить дырявый wu-ftpd, да еще и с поддержкой анонимного доступа, это прямо-таки экзотика. Найдя эксплоит для демона этой версии, взломщик натравил его на сервер. Через полчаса подбора адреса, вместо рутового шелла эксплоит выдал фатальное сообщение об ошибке. Но хакер не отчаивался и продолжал прощупывать жертву с разных сторон.

Время шло. Проверка демонов на неустойчивость особого успеха не принесла, но хакер уже располагал основными данными о них, а также об устройстве сервера в целом. Можно было подумать, что утро вечера мудренее, и закончить сбор данных. Но этот нарушитель сетевого порядка был не робкого десятка. Поэтому он и не думал сдаваться, а верил, что в любой каменной стене всегда найдется маленькая трещина.

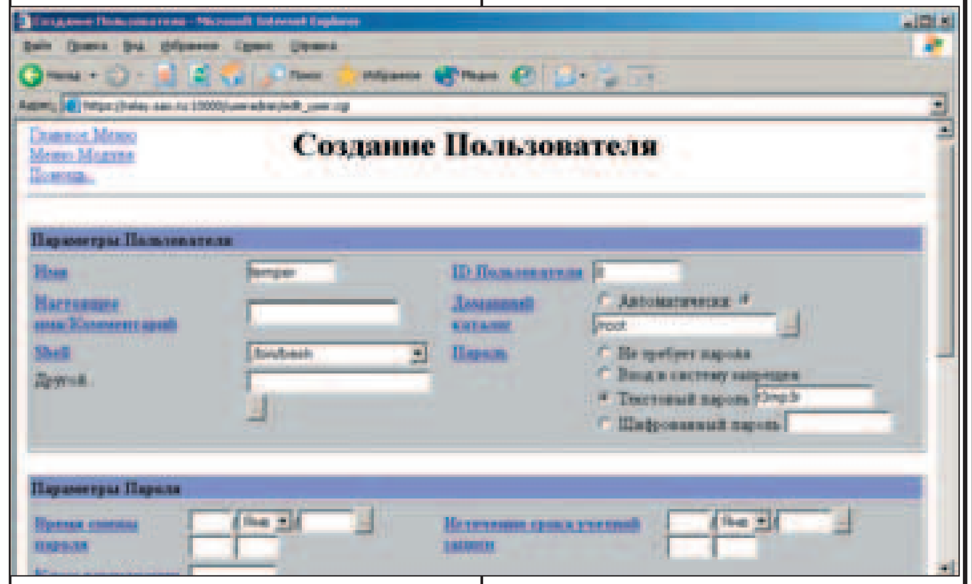
BRUTEFORCE - КЛАССИКА ВЗЛОМА

"Но что делать, когда такой трещинки не наблюдается?" - спросишь ты в надежде, что я выдам тебе секреты успехов великих хакеров. На самом деле, однозначно на этот вопрос ответить нельзя. Все зависит от ситуации. Наш же взломщик решил прибегнуть к самому опасному и неблагодарному методу - брутфорсу паролей. Вероятно, ты в курсе, что каждая попытка входа на сервер занимает довольно много времени (от секунды до пяти, в зависимости от пропускной способности канала). Но и это еще не все, ведь каждая попытка подбора пароля будет зафиксирована в логах.

Хакер определился, что подбирать пароль будет к системе web-управления сервером. Если ты посмотришь на список открытых портов, то, наверное, догадаешься, что на серваке присутствует Webmin. Для тех, кто в танке, расскажу, что это за система и с чем ее едят. Webmin - система, написанная на Perl и предназначенная для удаленного управления сервером через web. Она позволяет одним щелчком мыши ребутнуть сервер :) или посмотреть таблицу процессов, а также добавить нового пользователя, отредактировать конфиг и т.д. и т.п. Изначально Webmin придумывался для новичков-администраторов, которым легче управлять серваком через web, а не через SSH.

Наскоро написав простенький MIME-брутфорсер, наш герой натравил его на relay.sao.ru. Принцип работы этого брутфорсера очень прост: создается соединение с 10000 портом удаленного сервера. Затем осуществляется передача header'а с MIME-хешем ("login:password") и элементарный анализ возвращаемого результата (200 OK, либо 401 Error). Выбор сервиса Webmin был также неслучаен. Суди сам. Каждое соединение в Linux записывается в лог. В случае с хакером - /var/log/webmin.log. Если же выбрать сервис ftp, то попытки записывались бы в /var/log/messages - главный журнал системы. Риск обнаружения попытки взлома в этом случае оказался бы существенно выше. Во-вторых, был необходим действующий в системе логин. По опыту хакер знал, что большинство админов используют логин root для входа в Webmin, поэтому решил подбирать пароль именно к нему.

Через два часа интерактивный брутфорсер остановил перебор. "Закончился словарик", - подумал взломщик, но ошибся. Брутфорсер выполнил свою задачу, подобрав пароль для учетной записи root. Для справки: пароль был "digital", видимо тамошний админ был любителем цифровых технологий :). Далее шел стандартный алгоритм действий: создание пользователя с рутовыми правами (через Webmin), вход в систему через SSH и чистка логов за собой.



Создание пользователя через Webmin

ЧИСТКА ЛОГОВ

Логам наш герой уделял особое внимание. Он осознавал, что только через них админ сможет узнать о взломе сервера. Потратив около получаса на анализ /var/webmin/webmin.log, /var/log/messages, /var/log/secure, а также бинарного /var/log/wtmp, хакер стал изучать локалку в системе Sao. Ведь он всегда помнил, что www-сервер компании далеко не конечная цель. Впереди его ждала еще одна нелегкая работенка.

/sbin/ifconfig показал, что в системе существовали две локальные подсетки: 10.0.0.0/24 и 10.0.1.0/24. Но конечным объектом хакера был сервер с ip-адресом 10.0.1.35, поэтому на другие машины он попросту задвинул. Для дальнейшего изучения тачки 10.0.1.35 хакеру понадобился сканер. Он создал временную директорию /usr/man/info, скачал и установил в эту папку nmap (./configure --prefix=/usr/man/info).

ВЗЛОМ ЧЕРЕЗ SSH

После непродолжительного сканирования стало ясно, что за адресом 10.0.1.35 скрывается пингвин. Только вот открытых портов на нем было всего два: ssh и ftp. Взлом через ftp отпадал сразу - отсутствовала поддержка анонимного доступа. Хакеру оставалось лишь надеяться на удачу и изучать главный relay-сервер изнутри, либо использовать промежуточный взлом для проникновения на интересующую его машину. Использовать снифер он не хотел, т.к. знал, что при таком раскладе админы его обнаружат уже на следующее утро, да и заказчик платил только за срочную и качественную работу. Зайдя в рутовую директорию, хакер увидел там множество архивов с различным софтом, следовательно, админ своевременно апдейтил бинарники в своей системе. Файл /root/.bash_history показал, что системщик не зря получает зарплату, занимаясь исключительно полезным делом. Взломщик уже собирался уходить из владений рута, но шестое чувство заставило его выполнить команду find /root -type f для просмотра всех файлов в рутовой дире без исключения. Несмотря на нелепость этой команды, внимание взломщика привлек файл identity, лежащий в папке /root/.ssh. Тот, кто знает методы авторизации OpenSSH, уже догадался, что рут, как и все админы, был ленив и авторизовывался ключами. Плюс данного метода авторизации в том, что он не требует наличия пароля: обмениваясь ключами, sshd решает, пускать пользователя на сервер или нет. Чем же хакер хуже рута? Тем более ip-адрес 10.0.1.35 находился в known_hosts, значит, есть надежда, что админ и на этот сервер входит при помощи ключиков.

NEXT

Таблица 3

```
relay# ssh 10.0.1.35 -l root
Enter passphrase for RSA key
'root@relay':
bad passphrase given, try again...
^C
relay#
```

Взлом

ОБСЕРВАТОРНЫЕ ЗЛОДЕЯНИЯ

Master-lame-master

Опять неудача. Ключ все-таки был защищен фразой-паролем. Помянув недобрым словом всех родственников админа, хакер продолжил поиски путей проникновения на машину. Методы авторизации заставили его задуматься: ведь не только рут мог ходить по ssh, используя ключи. Команда locate identity показала, что ключи любил также некий пользователь sergey. Более того, в его known_hosts находился ip-адрес нужной машины.

```
relay# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:80:48:ED:84:5E
          inet addr:10.0.0.1  Bcast:10.10.0.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:151800 errors:0 dropped:0 overruns:0 frame:1
          TX packets:138660 errors:0 dropped:0 overruns:0 carrier:0
          collisions:149 txqueuelen:100
          Interrupt:11 Base address:0x240

eth1      Link encap:Ethernet  HWaddr 00:40:95:1C:7D:4D
          inet addr:10.0.1.1  Bcast:10.10.1.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1577369 errors:0 dropped:0 overruns:0 frame:6
          TX packets:303507 errors:0 dropped:0 overruns:0 carrier:0
          collisions:135 txqueuelen:100
          Interrupt:10 Base address:0x200
relay# ls -la /root/.ssh
total 57
drwx------    2 root     wheel         512 Apr 22 17:02 ./
drwxr-xr-x   17 root     wheel        1024 Apr 21 23:58 ../
-rw-r--r--    1 root     wheel        2419 Mar 26 18:19 authorized_keys
-rw-------    1 root     wheel         672 Mar 14 23:17 id_dsa
-rw-r--r--    1 root     wheel       49845 Apr 22 16:54 known_hosts
-rw-r--r--    1 root     wheel        1805 Feb 23  2002 known_hosts2
relay#
```

Детальный осмотр взломанного сервака

На этот раз фортуна улыбнулась нашему герою. После команды su sergey и ssh 10.0.1.35, хакер попал на интересующую его тачку. Судя по motd, этот сервер отводился под некую библиотеку астрофизической обсерватории. Теперь он догадался, почему заказчик не хотел отдавать свои документы в чужие руки. Все бы ничего, но нарушителю кибернетического порядка не понравилось, что в системе помимо него находились около десятка пользователей, в том числе и root (с www.sao.ru). Идл-тайм всех пользователей превышал час, поэтому тревога оказалась ложной (хотя хакер терпеть не мог, когда кроме него в системе находятся другие, пусть даже молчаливые личности :)).

ЯДЕРНЫЕ ОШИБКИ

В файле /etc/redhat-release взломщик нашел интересующие его сведения о системе - на компьютере был установлен RedHat 7.1. Операционка довольно стойкая, единственный ее изъян мог быть в ядре. Команда "uname -r" радостно сообщила, что ядро версии 2.2.18. Теперь хакер был уверен, что его работа практически выполнена. Ломать это ядрышко он решил известным публичным эксплоитом epcs2.c, предназначенным для <= 2.2.18 ядер. Интернет на машине закрывался фаерволом, поэтому эксплоит пришлось транспортировать командой /bin/cat с обычным перенаправлением ввода (см. скрин).

Параметром этого сплоита должна являться любая суидная программа. Хакер выбрал /usr/bin/passwd. Нетрудно догадаться, что буквально через секунду он получил полноценный root-shell в системе. Взломщику оставалось лишь войти в директорию /usr/biblio/docs, получить список каталога (чтобы доказать успешное выполнение работы) и удалить оттуда файлы, про которые говорил заказчик.

```
[sergey@biblio ~]$ cat > epcs2.c
/*
 * epcs2 (improved by lst [liquid@dqc.org])
 * ~~~~~~~
 * exploit for execve/ptrace race condition in Linux kernel up to 2.2.18
 *
 * originally by:
 * (c) 2001 Wojciech Purczynski / cliph / <wp@elzabsoft.pl>
 *
 * improved by:
 * lst [liquid@dqc.org]
 *
 * This sploit does _not_ use brute force. It does not need that.
 * It does only one attemt to sploit the race condition in execve.
 * Parent process waits for a context-switch that occur after
 * child task sleep in execve.

*** SKIPPED ***
[sergey@biblio ~]$ gcc epcs2.c -o epcs2
[sergey@biblio ~]$ ./epcs2 /usr/bin/passwd
bug exploited successfully.
enjoy!
[root@biblio sergey]# id
uid=0(root) gid=0(root) groups=100(users),111(biblio-adm),116(biblio)
[root@biblio sergey]#
```

Умело закачаем и применим эксплоит :)

ЕЩЕ ОДНА ЧИСТКА

Оставался последний штрих - чистка логов на двух взломанных серверах (следы от суидов, ssh-аутентификации и различных видов сканирования). И только после тщательной проверки на отсутствие оставленных временных папок и log-записей, хакер уничтожил временного юзера, созданного при помощи Webmin. Потом он гордо удалился, не причинив никакого вреда системе. Через несколько часов заказчику были предоставлены доказательства проделанной работы (список удаленных файлов). В итоге хакер получил слова благодарности и приличное вознаграждение. Как обычно - все счастливы.

Внимание! Этот материал не стоит расценивать как руководство взломщика. Его цель - указать администраторам на типичные уязвимости в их серверах. Своевременное обновление софта и настройка фаервола убережет систему практически от любого хакера :). Необходимо помнить об этом.

Что же помогло хакеру в его нелегком деле?

1. Взломщик не останавливается на одном методе. В нашем примере - сканировании. Более того, он использует даже такие небезопасные методы, как bruteforce, надеясь, что после взлома почистит за собой логи. Что сказать, риск - дело благородное.
2. Профессиональный взломщик сам пишет для себя софт, не надеясь на других! Если человек - хороший программер, то сложностей в реализации выбранного метода у него не возникнет.

Взлом

РУКОВОДСТВО ПО СОЗДАНИЮ ИНТЕРНЕТ-МАГАЗИНА

Докучаев Дмитрий aka Forb (forb@real.xakep.ru)



Ты с завистью смотришь на крупных бизнесменов, которые с легкостью зарабатывают себе на жизнь и тратят баксы направо и налево. Но ты никогда не задумывался, как устроить собственный бизнес. Устроить, не платить налоги и всегда быть при деньгах. Признайся, что ты всегда желал этого! И это не утопия, а вполне достижимая цель. Готовься, сейчас мы с тобой будем создавать многофункциональный интернет-магазин!

ЧТО ЖЕ НАС ЖДЕТ

Я вижу перед собой читателя с горящими глазами, мечтающего о легких деньгах и требующего описания всего и сразу. Не торопи события, мой друг, я расскажу все, что тебя интересует, но начну с самого начала. Итак, что же такое интернет-магазин? Человек, который браузит инет долгие месяцы, знает, что магазин (или попросту e-shop) - это обычный сайт, на котором выставлены на продажу различные товары (материальные или электронные). Сама реализация механизма выбора товара, онлайн продажи, заполнения корзины и т.п. осуществляется, как правило, при помощи скриптов.

Мы не будем создавать e-shop по продаже материальной продукции, более того, я даже не знаю, как это осуществить (сложные заморочки с бухгалтерией, почтовыми переводами, своевременной отсылкой товара и т.д. и т.п.). Намного проще создать магазин по продаже электронного товара, к примеру, shell-аккаунтов, icq номеров, email-баз и прочего. На самом деле, выбор электронной продукции огромен. Более того, налогами при этом виде коммерции можно пренебречь :).

Основные принципы магазина я описываю, опираясь на уже готовый и работоспособный проект itrade.pp.ru, ориентированный на продажу красивых шестизначных ICQ уинов. Почему itrade? Потому как, на мой взгляд, в этом e-shop'е интегрировано все, о чем я хотел бы рассказать. Но обо всем по порядку.

ДВИЖОК - ВСЕМУ ГОЛОВА

Для инет-магазинов существует множество универсальных движков. Все они выкладываются в глобал и доступны для скачивания. Но, порой, универсальность не приводит ни к чему хорошему. Живой пример: ты поставил на свой e-shop элитный движок, написанный неким Васей из Мухосранска. А на следующий день весь товар из твоего магазина наглым образом украли, оставив на память красивый дефейс. И все из-за того, что в движке Васи была бага, которая не раз обсуждалась в bugtraq.
Это я к тому, что движок, написанный своими руками, вероятно, будет намного надежнее проекта, взятого из инета. Пусть даже ты плохой программер, но твои скрипты никто не сможет изучить, поэтому взломать e-shop будет довольно проблематично.

Рассмотрим реализацию движка на itrade.pp.ru. Если немного побродить по сайту и потыкать на кнопочки, то несложно догадаться, что движок в своей работе использует MySQL. Более того, сам магазин написан на Perl, который интегрируется с базой данных без проблем. Взаимодействие достигается через модуль DBI. Для тех, кто не знает, напомню некоторые функции этого модуля.

После этого метод объекта $sth->fetchrow_arrayref вернет ссылку на массив, хранящий в себе вывод команды select. Работать с массивами в Perl, я думаю, ты умеешь (иначе открывай старые номера][или бегом в магазин за книжкой). В самой базе необходимо создать новую таблицу: с названием, ценой, описанием товара, а также статусом (продан/заказан/свободен). Всю эту информацию ты будешь отображать в HTML. Именно так реализован показ списка UIN'ов в моем примере. Например, заказ уина достигается путем изменения его статуса в MySQL-базе. После этого клиенту отправляется письмо с подтверждением. После успешной оплаты пароль от номера ICQ высылается клиенту на мыло (уже вручную, автором магазина).

Таблица 1

```
use DBI;
$dbh = DBI->connect("DBI:mysql:DataBase:ip-address",user,password); # Подключиться к базе DataBase, находящейся по адресу ip-address. Аккаунт для входа user:password
$dbh->do("update column set field=\"value\" where условие"); # Выполнить команду MySQL (insert, update, delete).

$sth=$dbh->prepare("select * from table where условие"); # Задать команду prepare
$sth->execute; # А затем выполнить ее
```

Непременный атрибут любого интернет-магазина - возможность его администрирования через web. Делается это элементарно: создается скрипт с основными функциями (добавление/удаление то-

вара и просмотр списка заказов). Затем реализуем все это при помощи основных функций работы с MySQL и защищаем паролем (на уровне httpd или скрипта).

ЖЕЛАНИЕ КЛИЕНТА ДЛЯ МЕНЯ ЗАКОН!

Как не крути, а клиент всегда прав. Поэтому не отчаивайся, если люди не будут покупать товар в твоем магазине. Возможно, их просто что-то не устраивает. Например, они не верят в твою честность и не согласны платить деньги, чтобы потом остаться без них и без товара. Так было и с нашим магазином по продаже ICQ номеров. Проблема решилась путем введения онлайн-оплаты через сервис Merchant компании Webmoney. Ты наверняка знаком с этой банковской компанией, через которую производится множество финансовых операций, в том числе и онлайн-оплата на сайтах. Сама оплата происходит следующим образом: после заполнения формы клиент попадает на сайт сервиса Merchant, который проводит авторизацию сертификатом. Затем с пользователя взимается определенная сумма денег, ее размеры задаются автором магазина. Если платеж прошел, браузер клиента перенаправляется на соответствующую ссылку, помеченную как success_url. В противном случае клиент попадает на failed_url (а не на бабки, как ты, наверное, подумал :)).

Если считаешь, что настроить такую систему крайне сложно, ты ошибаешься. Делается это за несколько минут. Вначале создаются два HTML документа, назовем их success.html и failed.html. Содержание их соответствует названию: первый документ будет судить о валидности платежа, второй документ появится, если платеж не пройдет. Затем напишем форму, результаты которой будут обрабатываться Merchant'ом.

Таблица 2

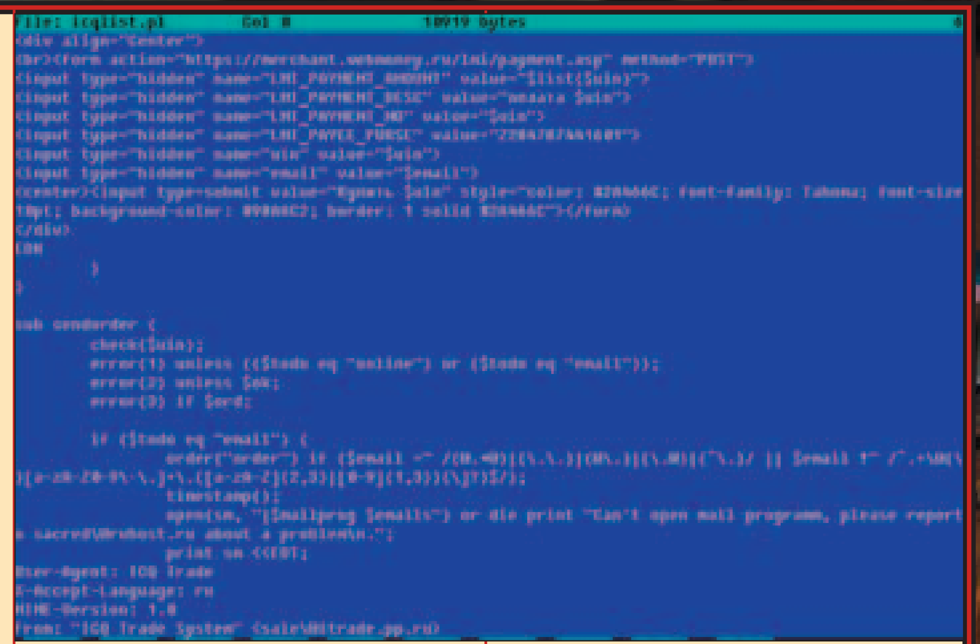
```
<form method="POST"

action="https://merchant.webmoney.ru/lmi/payment.asp">

<p>Купить Email базу за 1 WMZ</p>
        <input type="hidden"
name="LMI_PAYMENT_AMOUNT"
value="1.0">
        <input type="hidden"
name="LMI_PAYMENT_DESC" value="Покупка
E-mail базы">
        <input type="hidden"
name="LMI_PAYMENT_NO" value="1">
        <input type="hidden"
name="LMI_PAYEE_PURSE"
value="Z145179295679">
        <input type="hidden"
name="LMI_SIM_MODE" value="0">
        <input type="submit" value="submit">
</form>
```

Это пример самой короткой формы с основными и обязательными параметрами. Коротко скажу, что они означают:

LMI_PAYMENT_AMOUNT - сумма, которая должна быть перечислена на счет. Указывается с точностью до первого знака.
LMI_PAYMENT_DESC - описание платежа, будет



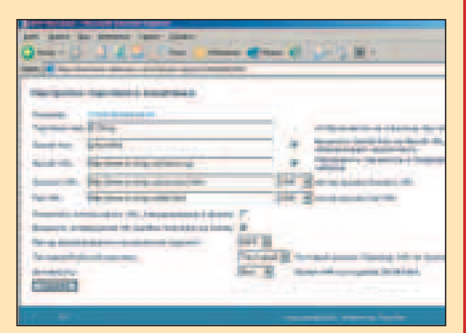
Форма с основными параметрами

высвечиваться в самом верху формы Merchant'a.
LMI_PAYEE_PURSE - кошелек, на который должен осуществиться перевод. Состоит из цифры (идентификатор валюты) и 12-значного кода.
LMI_SIM_MODE - режим работы системы. При значении 0 - режим тестовый, то есть система эмулирует нормальный перевод денег, но на самом деле счета остаются без изменений. Устанавливать рабочее значение 1 следует только в случае полной уверенности в правильной работе системы!

Теперь все готово. Осталось настроить Merchant для согласованной работы с твоей формой. Заходим на https://merchant.webmoney.ru, ползем в раздел "Настройка" и авторизуемся в WebMoney. Перед тобой появится форма, которую необходимо заполнить.

Торговое имя - подставь в это поле название своего проекта, чтобы пользователь знал, за что же он платит.
Secret Key - пароль для проведения оплаты. Поставь сюда любую последовательность символов.
Result URL - ссылка, на которую будут передаваться параметры платежа. Напиши значение http://your.e-shop.ru/cgi-bin/check_pay.cgi.
Success URL и Fail URL - соответственно ссылки на документы, которые ты составлял чуть выше.
Метод формирования контрольной подписи - MD5.
Тестовый/Рабочий режимы - тестовый (не изменяй, пока не убедишься в правильной работе системы!).





Корректно заполняем параметры формы

Таблица 3

```
use CGI qw(:standard);
use Digest::MD5
qw(md5_hex);

$LMI_PAYEE_PURSE=param('LMI_PAYEE_PURSE');
$LMI_PAYMENT_AMOUNT=param('LMI_PAYMENT_AMOUNT');
$LMI_PAYMENT_NO=param('LMI_PAYMENT_NO');
$LMI_MODE=param('LMI_MODE');
$LMI_SYS_INVS_NO=param('LMI_SYS_INVS_NO');
$LMI_SYS_TRANS_NO=param('LMI_SYS_TRANS_NO');
$LMI_SYS_TRANS_DATE=param('LMI_SYS_TRANS_DATE');
$LMI_SYS_TRANS_DATE=~s/\%3A/\:/g;
$LMI_SYS_TRANS_DATE=~s/\%20/ /g;
$LMI_PAYER_PURSE=param('LMI_PAYER_PURSE');
$LMI_PAYER_WM=param('LMI_PAYER_WM');
$lmihash=param('LMI_HASH');

## Берем все параметры из
QUERY_STRING.

$LMI_SECRET_KEY="password"; ##
Секретная фраза должна совпадать с
фразой на Merchant'e
$data=$LMI_PAYEE_PURSE.$LMI_PAYMENT_AMOUNT.$LMI_PAYMENT_NO.$LMI_MODE.$LMI_SYS_INVS_NO.$LMI_SYS_TRANS_NO.$LMI_SYS_TRANS_DATE.$LMI_SECRET_KEY.$LMI_PAYER_PURSE.$LMI_PAYER_WM; ## Склеиваем строку,
состоящую из этих параметров

$lmihash=lc($lmihash); ## Понижаем
регистр возвращенного хеша.
$myhash=md5_hex($data); ## И кодируем
свой.

exit 0 unless ($lmihash eq $myhash); ##
Выходим, если подписи не соответствуют
## Иначе продолжаем работу.
```

Докучаев Дмитрий aka Forb (forb@real.xakep.ru)

Движки для интернет-магазинов

Если нет желания кодить движок для интернет-магазина самому, тебе в этом поможет множество фирм. Все их можно найти через поисковик. Живым примером такой фирмы является проект http://www.dezi.ru.

ДОВЕРЯЙ, НО ПРОВЕРЯЙ!

Система платежей бесспорно надежна, но от лишней проверки хуже никому не станет. Как ты думаешь, почему я указал ссылку на несуществующий скрипт check_pay.cgi в параметре Result URL? Потому что сейчас мы займемся кодингом и составим этот скрипт, задачей которого будет доведение процесса до автоматизма - проверка MD5-подписи и отсылка оповещающего e-mail клиенту. Не буду тебе пересказывать изнуряющие мануалы Merchant'а, скажу только, что проверка ключа происходит путем сравнения параметров, заданных в скрипте и приходящих через QUERY_STRING. Для корректной работы, нам понадобится модуль Digest::MD5 (он поставляется с дистрибутивом Perl). Вот краткий код скрипта:(таблица 3)

Таблица 4

```
$lmihash=lc($lmihash); ## Понижаем регистр возвращенного хеша.
$myhash=md5_hex($data); ## И кодируем свой.

exit 0 unless ($lmihash eq $myhash); ## Выходим, если подписи не соответствуют
## Иначе продолжаем работу.
```

Далее действуй в зависимости от ситуации. Можешь отправить письмо клиенту. Для этого воспользуйся sendmail'ом, либо сокетами (этому тебя не раз учили в рубрике Кодинг).

Если использовать Perl не представляется возможным, то делай магазин на PHP или вообще при помощи одних HTML-документов. Правда, в поле Result URL нужно внести ссылку в качестве e-mail адреса (все параметры о платеже придут тебе на e-mail) в форме "mailto:root@e-shop.ru". Тем более, взломать твой "HTML-движок" будет невозможно ;).

Пришло время добавить ложку дегтя в бочку меда. Ситуация такова: Merchant в полном режиме будет доступен лишь тем, у кого есть персональный аттестат доверия. Этот аттестат можно получить в любом крупном городе, предоставив свои паспортные данные. Это было сделано в связи с участившимися случаями обмана клиентов. Радует лишь, что цена такого аттестата колеблется от 3 до 10 баксов. Я думаю, что отдать 300 деревянных рублей за благое дело не будет для тебя большой проблемой.

WebMoney transfer

Для выполнения прямого платежа на кошелек продавца нажмите кнопку **Оплатить** и пройдите авторизацию в системе. Вы увидите все детали платежа на экране и сможете подтвердить или отменить платеж. Для выполнения платежа вы должны быть зарегистрированы в системе WebMoney Transfer

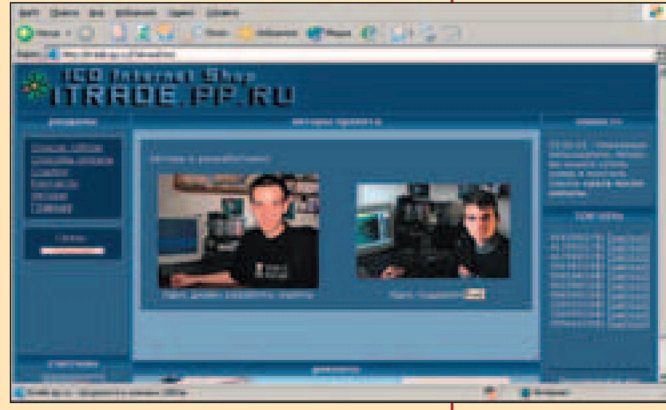
прямой платеж на кошелек продавца

счет #	416200
на сумму	17.00
на кошелек	Z284787441601
продавец	ICQ Trade
WMId:	780771962335 проверить аттестат
название товара/услуги	оплата 416200

[Оплатить] [Отказаться от оплаты]

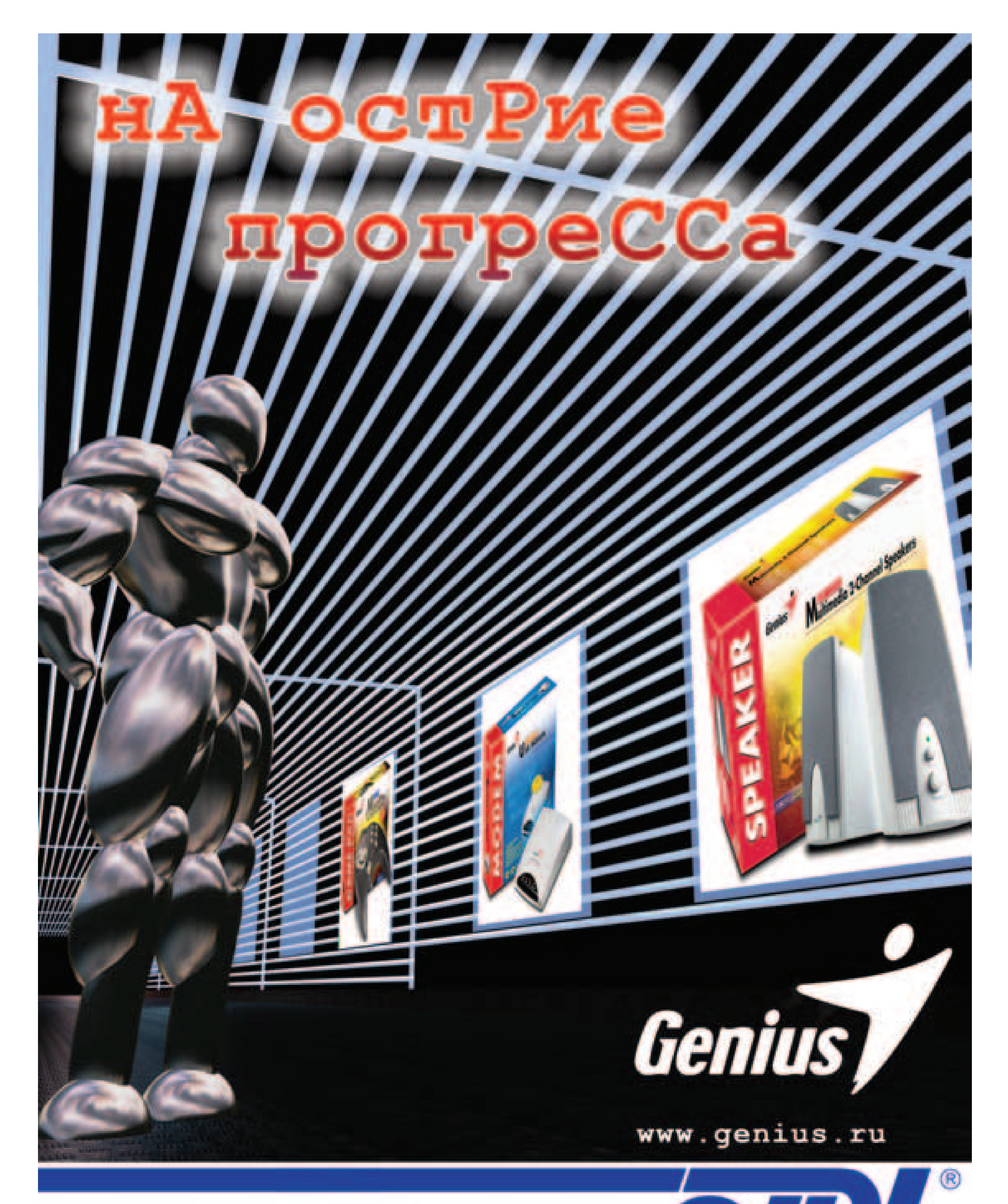
Корректно заполняем параметры формы

Itrade.pp.ru не исключение. У этого магазина есть свой аттестат доверия, и все операции со счетами проводятся законно. Более того, авторы магазина всегда действуют в интересах клиентов, поэтому цены на товар периодически снижаются. На правах рекламы, приглашаю всех заинтересованных лиц заглянуть в наш скромный e-shop :).



Наш небольшой e-shop

Мораль сей басни: интеграция Perl и MySQL на порядки упрощает работу с крупными проектами. А если к этому прибавить Merchant, то тебе совершенно не придется заботиться о способах оплаты ;), просто вовремя пополняй товар и получай легкие деньги.


нА остРие
прогреСCа
SPEAKER
Genius
www.genius.ru

Взлом

ОТКРЫТЬ ВОРОТА!

Туткабаев Еркебулан (streetseeker@mail.ru)

ОТКРЫТЬ ВОРОТА!

СВЯЗКА КЛЮЧЕЙ К МОЗГУ ЛОКАЛКИ - МАРШРУТИЗАТОРУ

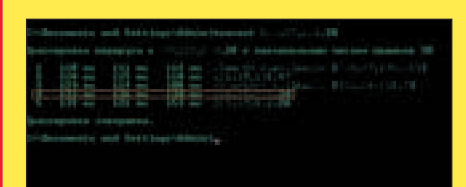
В прошлом номере мы разбирали основы работы маршрутизаторов. В этой же статье я расскажу о том, как же ломают эти роутеры, какие бонусы можно поиметь от такого хака, и опишу конкретную методику его овладением. И напоследок - кучку багов от наиболее широко распространенных моделей маршрутизаторов.

Многие полагают, что единственный способ администрирования роутера заключается в подсоединении к нему толстенного кабеля с последующими стандартными мучениями с прилагаемым софтом. Так вот! Большинство роутеров имеют встроенный telnet, то есть их можно "настроить" удаленно :). Это обстоятельство сильно помогает хакеру в его темном деле - не придется фехтовать с админом на ножках от стула. Только послушай, что даст взломщику прирученный роутер - как и положено серьезному сетевому устройству, он имеет под собой нехилую скорость. Отсюда следует, что для сноса кого-нибудь пингом уже не придется лазить на шелл - раз. Ежесекундно сквозь него проходят мегабайты данных, которые реально поснифать - два. Маршрутизатор имеет свой IP-адрес, и с ним могут быть установлены доверительные отношения - три. Через его telnet-интерфейс можно ломать дальше, подставляя IP роутера - четыре. Так что взлом маршрутизатора - это серьезно, а стадо подобных подломанных девайсов - еще серьезней. Но довольно слов, давай ближе к делу. Из инструментария хакеру понадобятся следующие проги: Telnet, HyperTerminal, Ping, Tracert, пара проксей с telnet-доступом. Все вышеперечисленные программы находятся в стандартной поставке виндов, единственный напряг могут вызвать проксики. Их обычно тестируют на прозрачность.
А теперь пошла загрузка текста в мозг...

SEARCHING… 68% COMPLETE

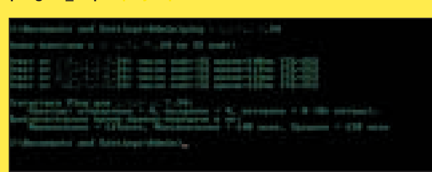
Самый легкий шаг на пути покорения роутеров - это обнаружение роутера. Если хакер вконец обнаглел и собирается ломать собственного провайдера :), то он просто отдает следующую команду:

```
tracert IP_адрес_любого_сайта
```



Командная строка с темно-зеленым текстом со статистикой для tracert

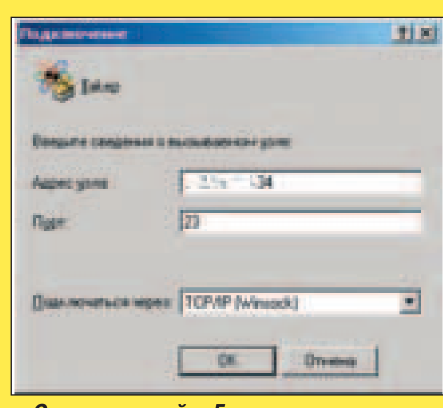
Tracert позволяет показать злодею весь маршрут пакета до пункта назначения. Его пров обязательно держит какой-либо маршрутизатор, и его IP высветится в статистике для traceroute. Возможно, он будет иметь имя Cisco. В моем случае пров оказался упертый, и кроме IP я ни черта не увидел, пришлось пробивать вручную. Далее нужно проверить, прячется ли роутер за фаерволом. Для этого следует не менее простая команда - ping IP_адрес роутера.



Командная строка статистикой для ping

Здесь все просто - если ответ приходит, то велика вероятность того, что фаервола нет. Окончательно решает вопрос о существовании фаера коннект Telnet'ом на роутер (порт 23).

Если у хакера запрашивают логин, то увы - фаервол на страже, а про обход фаерволов - в следующий раз :(. Но взломщик перец фартовый, так что должно прокатить. Итак, если у нашего героя, НЕ спрашивая логина, запрашивают пароль, то он уже у входа в роутер. Осталось сделать один шаг, но здесь есть нюанс - на роутере должен стоять софт версии 4.1. Зажмурив глаза, набивает пароль... Какой? Зачем ему забивать себе этим голову – главное, чтобы он был большой, не менее 250 символов :). Обалдев от такого пасса, система валидации накрывается, позволяя вломиться в его кишки: забивание в качестве пароля "admin" (без кавычек, разумеется). Теперь, когда хакер в системе, осталось лишь угнать файл паролей. Он быстренько вытаскивает на свет божий HyperTerminal, настраивает новое соединение. В поле "Подключаться через" ставит TCP/IP (Winsock).



Окошко настройки Гипертерминала

В строке адрес взломщик забивает адрес атакуемой тачки, порт - 23. На роутере получает хелп по командам "?" (в роутерах команды разнятся, так что придется ориентироваться на местности), быстро листает файлы и отправляет на свой IP на порт 23 все подозрительные :). HyperTerminal спросит его, стоит ли принимать файлы, на что, разумеется, надо ответить "Да". Теперь отваливает из сети и, не спеша, наслаждаясь каждой секундой, скармливает файлы любимому Джонни (John The Ripper). Все! Теперь одним рабом в сети стало больше ;). Но мерзкий хакер помнит, что лень админов ему только на руку, да и совковое мышление все еще рулит - ну не может наш человек понять, что железо тоже можно обновлять через сеть.

Telnet нам в помощь

Как ты, наверное, знаешь, весь основной хак роутеров происходит с использованием стандартнейших прог виндов, что, несомненно, должно порадовать будущего хакера-ленивца :). Как я упоминал в прошлом номере, основная тупость админов как была, так и остается одной: использование паролей по дефолту и нежелание обновлять ПО. Ты не поверишь, насколько часто, по роду своей профессии, я сталкиваюсь с этими ламаразмами. Так что хакеру рекомендуется раздобыть хороший список дефолтовых паролей для роутеров, в сети их предостаточно. Также хакера может ломать что-либо делать вообще, и он хочет просто замочить зло-роутер, тогда в атаку идут эксплоиты. Вот пример одного: http://packetstormsecurity.org/cisco/cisconuke.c. По завершении компиляции получится нюкер для роутеров от Cisco :).

ОДИН БАГ ХОРОШО, А N! БАГОВ ЛУЧШЕ

Теперь галопом по Европам. Вот кучка багов с общей концепцией эксплоитинга. Свитчи Cisco Catalyst 5000 Series Ethernet, Catalyst 1200, Catalyst 2900, Catalyst 5500. Посылая на открытый порт символ возврата каретки, хакер заставляет его размышлять о смысле бытия :).

Любой роутер от Cisco, на котором включена фича IOS HTTP. Попробовав постучать на http://<ip-routera>/%%, получаешь нокдаун роутера.

Cayman 3220-H DSL Router. Как и в вышеописанном случае, в бой пошли большой логин и гигантский пароль. Роутеру этого будет достаточно.

Cisco 2500 Series. Банальный флуд. Шлешь кучу UDP-пакетов с левыми обратными адресами на порт #7.

Любая циска с IOS 11.2A и с любой версией из трэйла 12.0.x. Здесь та же песня: куча битых UDP-пакетов на порт #514 и - вуаля.

Cisco Secure Access Control Server для виндов. Сервис на порту #2002 подвержен переполнению буфера. Комментарии излишни :).

Роутер NB1300: FTP-сервер с WAN-интерфейсом. То ли пасс сменить гиморно, то ли еще что-то, но факт - я еще не встречал таких роутеров с логином и паролем, отличными от admin:password :).

Команда "get config.reg" - и логин с паролем для роутера у взломщика в руках. В смысле - в открытом тексте :).

Уязвимость была обнаружена в маршрутизаторах модели D-Link DSL Broadband Modem. Установка программного обеспечения по умолчанию устанавливает и активизирует службу SNMP (Simple Network Management Protocol) с общими именами, оставленными по умолчанию. Если создать Telnet-сессию и войти в систему с именем "public", то можно получить доступ с правами чтения всех чувствительных данных о сети. Если же войти с именем "private", то получаешь полный доступ чтения/записи ко всем параметрам маршрутизатора.

U.S.Robotics Broadband-Router 8000A. Уязвимость находится только в данной модели маршрутизатора, основана она на неправильной обработке исключительных ситуаций. Открыв Telnet-сессию с маршрутизатором и отдав ему GET-запрос, можно будет удаленно завершить работу маршрутизатора и перезагрузить его.

Shiva AccessPoint routers. Тут народ отрыл прикольную фичу - после отсылки UDP-пакета, в качестве полезной нагрузки которого находится следующая строка: 44 49 52 4b 02 01 01 00 (тут пишешь потребный IP-адрес в HEX), адрес роутера изменится НА УКАЗАННЫЙ. Правда, круто? :)

Cisco UBR900. Здесь тот же прикол, что и в D-Link. Используя вышеуказанные сетевые имена, можно будет получить полный доступ к настройке IOS. Похоже, что код для обоих роутеров писал один и тот же человек.

Опять же, на практике я не раз видел, что ряд роутеров хранят пароли в открытом виде (в конфигурационном файле), так что если у хакера есть физический доступ к роутеру, то имеет смысл пошерстить его файлы на предмет пассов...

Роутеры от Cisco. Юзая строчку http://ip_routera/level/chislo/exec/... (где chislo - цифра между 16 и 99), можно получить полный админовский доступ.

Вот, в общем-то, и все. Это одни из самых распространенных ошибок. Ими хакеры и пользуются в своих мерзких злодеяниях. Так что, если ты являешься админом какой-нибудь сетки с роутерами, тебе стоит призадуматься, все ли у тебя грамотно настроено. Поэтому впитывай полученную информацию, и вперед, добиваться новых высот в плане безопасности!

Ахтунг!

Хочу предупредить, что если ты захочешь применить эти знания на практике на какой-нибудь чужой тачке, ты попадаешь под УКРФ. Так что за последствия применения того, что здесь написано, будешь нести ответственность ты и только ты. Все нижеследующее можно использовать только в образовательных целях и только в своей локалке :). Внял? А теперь понеслось!

Взлом

ПРОВАЙДЕР В ДОМАШНИХ УСЛОВИЯХ

Andrushock (andrushock@real.xakep.ru)



ВСЕ ЧТО ТЫ ХОТЕЛ ЗНАТЬ О НАСТРОЙКЕ DIALIN-СЕРВЕРА

Еще пару лет назад никто не мог предположить, что объемы передаваемой информации настолько возрастут, модемной скорости будет не хватать, а эти чуждые прежде слова: ISDN, Frame Relay, радиолинк будут ласкать наш слух и станут родными. Вот, наверное, уже и у тебя в школе/универе/конторе обзавелись выделенным каналом. Хмм… Ты еще не придумал, как этим можно выгодно воспользоваться? Тогда давай я тебе немного помогу: два модема, халявный трафик, удаленный доступ по расписанию, пиво с друзей. Если у тебя после прочтения последних слов загорелись глаза, участилось сердцебиение, закивала голова :), то быстрее доставай парочку модемов - сегодня мы замутим свой собственный одноканальный модемный пул!

<СХВАТКА №1: PPP VS SLIP>

В настоящее время протокол двухточечного соединения PPP (Point-to-Point Protocol), предназначенный для передачи IP-пакетов через последовательную связь, пришел на смену более медленному и менее эффективному протоколу SLIP (Serial Line Internet Protocol - межсетевой протокол для последовательного канала) и CSLIP (Compressed SLIP - протокол SLIP с возможностью сжатия TCP заголовков всего до трех байт), давно разработанных Риком Адамсом и Ваном Джекобсоном.

Протокол PPP состоит из трех элементов:
- протокола HDLC (High-level Data Link Control - управление передачей данных высокого уровня), определяющего структуру и 16-битную контрольную сумму PPP-пакетов;
- протокола LCP (Link Control Protocol - протокол управления каналом), занимающегося согласованием опций, установлением и тестированием соединения на канальном уровне;
- протокола NCP (Network Control Protocol - протокол управления сетью), необходимого для взаимодействия с сетевыми протоколами.

Для работы PPP используются следующие три компонента операционной системы:
- драйвер HDLC (входит в ядро ОС), управляющий потоком данных по каналу связи;
- демон pppd, выполняющий основные функции PPP;
- утилита chat, используемая для установки соединения - набора номера абонента в автоматическом режиме.

К недостаткам протокола PPP можно отнести ненадежность канала, довольно низкую скорость передачи данных (до 56 Кбит/сек) и существенное ограничение на количество компьютеров - всего лишь два хоста способны одновременно участвовать в сеансе связи по этому протоколу (собственно, поэтому создать локальную сеть, используя этот протокол, никоим образом не удастся, несмотря на то, что PPP обеспечивает все функциональные возможности Ethernet).

<СХВАТКА №2: PAP VS CHAP>

Для аутентификации пользователей по протоколу PPP обычно используется один из двух типов опознавания - это PAP (Password Authentication Protocol - протокол парольного опознавания), либо CHAP (Challenge Handshake Authentication Protocol - протокол опознавания вызова установления связи).

При использовании первого протокола не происходит ничего сверхъестественного: клиент отправляет свою учетную запись и пароль серверу, который сравнивает их с записями либо из своей базы данных (файл /etc/ppp/pap-secrets, пароли хранятся plaintext'ом), либо с помощью функции crypt() с записями из теневого файла паролей операционной системы (/etc/shadow в Linux и Solaris, /etc/master.passwd в Free/Net/OpenBSD).

Работа по протоколу CHAP происходит гораздо интересней: сервер высылает клиенту вместе со своим именем хоста рандомно сгенерированный секретный ключ. Клиент, получив имя и ключ, на их основе создает, в свою очередь, собственный шифр и возвращает его для опознавания серверу, и только после этого происходит вход пользователя в систему. Во время сеанса, через определенные промежутки времени, сервер генерит и посылает клиенту ключики, а затем сверяет полученные хэши, чтобы убедиться в его (клиента) подлинности. Однако в системе пароли пользователей хранятся открытым текстом в файле /etc/ppp/chap-secrets.

Все же, несмотря на некоторые преимущества CHAP, подавляющее большинство провайдеров до сих пор используют протокол PAP. Как правило, CHAP чаще применяют для аутентификации клиентов для получения доступа в виртуальные частные сети.

<СХВАТКА №3: GETTY VS MGETTY>

При загрузке операционной системы одной из главных функций демона init является порождение отдельного процесса специальной программы getty (сокращение от двух слов "get tty" - "получить tty"), которая устанавливает характеристики последовательных устройств, выдает на экран монитора prompt (регистрационное приглашение) и

переходит в режим ожидания - пока пользователь не введет имя своей учетной записи и пароль. Затем getty, чтобы пользователь смог получить доступ к командному интерпретатору, запускает программу login, передавая ей в качестве аргумента идентификатор пользователя. Также getty умеет конфигурировать модулятор-демодулятор и ожидать входящие подключения. Параметры getty и типы терминалов демон init берет из системных конфигурационных файлов /etc/{inittab, ttytype, gettydefs} в Linux или /etc/{ttys, gettytab} в BSD.

Как видишь, getty выполняет довольно много задач, но, к сожалению, плохо поддерживает модемы. Поэтому Гертом Дорингом была создана программа mgetty - модифицированная версия getty, специально ориентированная на работу с Hayes-совместимыми модемами. К тому же mgetty поддерживает функцию голосовой почты, прекрасно справляется с получением факсов и, по сравнению с getty, легче конфигурируется. Обратной стороной медали в использовании mgetty является безопасность. Команда OpenBSD в своем дереве портов пометила mgetty как BROKEN с не нуждающимся в переводе комментарием: "insecure tempfile handling: can overwrite any file on the system". Стоит отметить, что и getty, и mgetty понимают протоколы PAP и CHAP.

Рассмотрев вышеописанные плюсы и минусы, взвесив все за и против, остановимся на следующей конфигурации: будем соединяться по протоколу двухточечного соединения PPP, применять PAP аутентификацию и использовать инсекьюрную mgetty. А в качестве операционки рулить у нас будет пингвинятко Тукс.

<ЯДЕРНЫЕ ИНГРЕДИЕНТЫ>

Прежде чем разбираться с софтом для настройки сервера dialin, нужно выяснить, скомпилировано ли ядрышко подопытной системы со всеми необходимыми опциями. Кроме того, крайне желательно для гибкости нашей конфигурации и уменьшения размеров ядра включить поддержку PPP в виде модуля. Преимущества такого подхода особенно очевидны на и без того активно swap'ующихся машинах. Модули ядра будут загружаться и выгружаться из драгоценной памятки только при необходимости, освобождая под повседневные задачи хоста максимальное количество оперативки.
Итак, забираем с http://www.kernel.org/ последнее стабильное ядро ветки 2.4, распаковываем в каталоге /usr/src полученный архив:

```
# bunzip2 < linux-2.4.20.tar.bz2 | tar xvf -
```

Переходим в созданный каталог и начинаем конфигурирование ядра:

```
# make mrproper
# make menuconfig
```

Добавляем в ядро возможность использования загружаемых модулей; поддержку работы сети, протокола TCP/IP, специальных устройств, сам протокол PPP и методы сжатия (см. Врезку 1).

Далее вырабатываем файл зависимостей, удаляем временные и объектные файлы, создаем сжатый образ ядра, компилируем и устанавливаем модули:

```
# make dep clean bzImage modules modules_install
```

Копируем свежеиспеченный кернел вместе с map файлом в загрузочный каталог, не забывая затем озадачить бут менеджер новым ядром:

```
# cp arch/i386/boot/bzImage /boot/vmlinuz-2.4.20
# cp System.map /boot/System.map-2.4.20
# rm -f /boot/System.map
# ln -s /boot/System.map-2.4.20 /boot/System.map
# vi /etc/lilo.conf
# /sbin/lilo -v
```

```
Realtek 8169 Gigabit Ethernet support (CONFIG_R8169) [M/n/y/?] n
SysKonnect SK-98xx and SK-95xx Gigabit Ethernet Adapter family support (CONFIG_S
K98LIN) [M/n/y/?] n
Broadcom Tigon3 support (CONFIG_TIGON3) [M/n/y/?] n
FDDI driver support (CONFIG_FDDI) [Y/n/?] n
Network logging support (CONFIG_NETCONSOLE) [M/n/y/?] n
HIPPI driver support (EXPERIMENTAL) (CONFIG_HIPPI) [N/y/?] n
PLIP (parallel port) support (CONFIG_PLIP) [M/n/?] n
PPP (point-to-point protocol) support (CONFIG_PPP) [M/n/y/?]
  PPP multilink support (EXPERIMENTAL) (CONFIG_PPP_MULTILINK) [Y/n/?] n
  PPP filtering (CONFIG_PPP_FILTER) [Y/n/?] n
  PPP support for async serial ports (CONFIG_PPP_ASYNC) [M/n/?]
  PPP support for sync tty ports (CONFIG_PPP_SYNC_TTY) [M/n/?] n
  PPP Deflate compression (CONFIG_PPP_DEFLATE) [M/n/?]
  PPP BSD-Compress compression (CONFIG_PPP_BSDCOMP) [M/m/?]
  PPP over Ethernet (EXPERIMENTAL) (CONFIG_PPPOE) [M/m/?]

CONFIG_PPPOE:

  Support for PPP over Ethernet.

  This driver requires the current pppd from the "ppp" CVS repository
  on cvs.samba.org.  The required support will be present in the next
  ppp release (2.4.2).
  PPP over Ethernet (EXPERIMENTAL) (CONFIG_PPPOE) [M/m/?] _
```

Ядерный PPP

Осталось только сопоставить в файле /etc/modules.conf загружаемые модули с именами устройств (см. Врезку 2).

<КОМПИЛЯЕМ С УСПЕХОМ>

Все, с ядром разобрались. Теперь переходим к инсталляции программного обеспечения на пользовательском уровне, а именно к установке ppp и mgetty. Для начала проверь, все ли необходимые пакеты у тебя есть:

```
$ rpm -qa | grep ppp
$ rpm -qa | grep mgetty
```

Если по какой-то причине таковые в системе отсутствуют, устанавливаем:

```
# rpm -Uvh ppp-2.4.1-7.i386.rpm
# rpm -Uvh mgetty-1.1.28-9.i386.rpm
```

А следующие хинты предназначены специально для сорвиголов, которые решили пойти по пути наибольшего сопротивления и собрать все ручками: 1) после слива софта с ftp://cs.anu.edu.au/pub/software/ppp/ http://alpha.greenie.net/mgetty/ и распаковки архивов, перед процессом компи-




```
LOADABLE MODULE SUPPORT --->
ENABLE LOADABLE MODULE SUPPORT (CONFIG_MODULES) [Y]
SET VERSION INFORMATION ON ALL MODULE SYMBOLS (CONFIG_MOD-
VERSIONS) [Y]
KERNEL MODULE LOADER (CONFIG_MODVERSIONS) [Y]

GENERAL SETUP --->
NETWORKING SUPPORT (CONFIG_NET) [Y]

NETWORKING OPTIONS --->
        TCP/IP NETWORKING (CONFIG_INET) [Y]

NETWORK DEVICE SUPPORT --->
NETWORK DEVICE SUPPORT (CONFIG_NETDEVICES) [Y]
DUMMY NET DRIVER SUPPORT (CONFIG_DUMMY) [Y]
PPP (POINT-TO-POINT) SUPPORT (CONFIG_PPP) [M]
PPP SUPPORT FOR ASYNC SERIAL PORTS (CONFIG_PPP_ASYNC) [M]
PPP DEFLATE COMPRESSION (CONFIG_PPP_DEFLATE) [M]
PPP BSD-COMPRESS COMPRESSION (CONFIG_PPP_BSDCOMP) [M]
```

Взлом

ПРОВАЙДЕР В ДОМАШНИХ УСЛОВИЯХ

Andrushock (andrushock@real.xakep.ru)

```
• ALIAS PPP0 OFF
• ALIAS CHAR-MAJOR-108      PPP_GENERIC
• ALIAS /DEV/PPP            PPP_GENERIC
• ALIAS TTY-LDISC-3         PPP_ASYNC
• ALIAS PPP0                PPP_GENERIC
• ALIAS PPP-COMPRESS-21     BSD_COMP
• ALIAS PPP-COMPRESS-24     PPP_DEFLATE
• ALIAS PPP-COMPRESS-26     PPP_DEFLATE
```

ляции ppp нужно указать, что в системе применяются теневые пароли плюс задать дополнительный аргумент для корректной работы Windoze-клиентов:

```
$ ./configure
$ make HAS_SHADOW=1 USE_MS_DNS=1
# make install
```

2) чтобы диалапщики логинились, минуя терминальное окно, в сырцах mgetty в правиле сборки Makefile к опциям компилера добавляем флажок -DAUTO_PPP:

```
CFLAGS=-O2 -Wall -pipe -DAUTO_PPP
```

Однако такого рода программы всегда лучше ставить из пакетов/пакаджей/портов, так как разработчики дистрибутивов занимаются не только хаотичным тасованием бинариков по всей файловой системе, но и производят аудит кода, отлавливают баги различной серьезности, тестируют тулзы на совместимость и работоспособность.

```
root@isengard:~
File  Edit  View  Terminal  Go  Help
[root@isengard root]# rpm -Uvh hsflinmodem-5.03.27mbsibeta02122000k2.4.18_14-1rh
.i686.rpm
Preparing...                ########################################### [100%]
   1:hsflinmodem            ########################################### [100%]
Linux HSF softmodem drivers, version 5.03.27mbsibeta02122600

WARNING: this is an EXPERIMENTAL BETA VERSION of the HSF drivers for Linux.
USE AT YOUR OWN RISK! See the file /usr/lib/hsf/LICENSE for details.

Conexant Systems neither distributes nor maintains this package.
PLEASE DO NOT CONTACT CONEXANT REGARDING THIS SOFTWARE!!!
If you require assistance or need more information, go to:
        http://www.mbsi.ca/cnxtlindrv

Selected PCI VendorID=14F1 DeviceID=2F12
and INF file /etc/hsf/inf/linux_hsf.inf

Configuring modem for country: "RUSSIA"
You can change this setting later with the command "hsfconfig --country"

Pre-built HSF modules that seem compatible with your system were found under
/usr/lib/hsf/modules/binaries/i686/RedHat/linux-2.4.18-14.

Your HSF modem should now be accessible as /dev/ttySHSF0
```

Для софтмодемов еще понадобятся дрова

<ПОРТИМ СИСТЕМНЫЕ КОНФИГИ>

Для начала разберемся, что же у нас творится с конфигурационными файлами mgetty:

```
$ ls /etc/mgetty+sendfax
dialin.config  login.config  mgetty.config
```

Первый из них не представляет для нас никакого интереса, во втором должна быть всего лишь одна строчка:

```
# vi /etc/mgetty+sendfax/login.config

/AutoPPP/ -    a_ppp   /usr/sbin/pppd file
/etc/ppp/options
```

Третий будет содержать все опции, которые необходимо передать mgetty:

```
# vi /etc/mgetty+sendfax/mgetty.config

debug 5                                    #
указываем степень журналирования
port ttyS0                                 #
определяем, к какому порту подключен наш модем
speed 57600
# скорость порта

data-only y                                #
факсимильная поддержка не требуется
init-chat "" ATZ OK ATS0=1 OK # строка инициализации модема
```

Команда ATS0=1 как раз указывает, что при входящем звонке модем должен брать трубу. Альтернативным вариантом будет использование ключевого слова "answer-chat", к примеру:

```
init-chat "" AT OK ATZ OK
answer-chat "" ATA CONNECT \c \r
```

При желании это можно сократить до:

```
init-chat "" ATZ OK
answer-chat "" ATA
```

Для того чтобы mgetty подцепила и сконфигурировала наш модем, в файле описания различных режимов работы операционки нужно добавить запись, содержащую идентификатор (можно указать любой - он используется как комментарий для удобства), уровни исполнения, активность mgetty, путь до бинарика mgetty и асинхронный последовательный порт, к которому подключен наш высокоскоростной модем.

```
# vi /etc/inittab

S0:345:respawn:/sbin/mgetty /dev/ttyS0
```

И заставим демона init перечитать /etc/inittab:

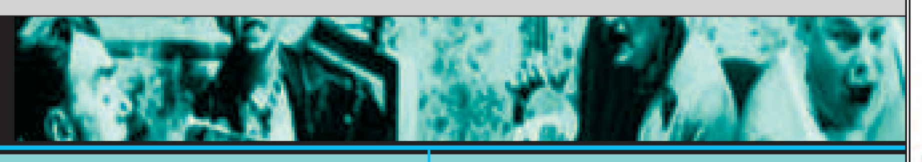
```
# init q
```

После этой команды должен загореться (естественно, если модем внешний) светодиод TR (либо MTR, в зависимости от модели и производителя) - это значит, что mgetty правильно подхватил модем и мы на верном пути. Теперь, для контрольного теста, попробуй позвонить на модем. Он должен при первом же гудке снять трубу и начать соединение. Если этого не произошло, то начинай разгребать /var/log/messages, /var/log/mgetty.log.ttyS0 и выяснять причину.

Осталось совсем немного - законфигурить pppd и добавить юзверей. Приступаем:

```
# vi /etc/ppp/options

// указываем, какие управляющие символы преобразовывать в Esc-последовательность
asyncmap 0
// требуем от клиента аутентифицироваться, используя PAP/CHAP
auth
// применяем аппаратный протокол установления связи через /dev/ttyS0
crtscts
// не будем переходить в фоновый режим
-detach
// создаем файл блокировки для последовательного устройства
lock
```



```
// используем теневой файл с паролями для PAP
login
// используем все сигналы управления модемами
modem
// отменяем поддержку CHAP
-chap
// только PAP
+pap
// стандартные твики диалапщиков
mtu 576
mru 576
// заставляем локальный хост отправлять все запросы от имени клиента
proxyarp
// отключаем неиспользуемые протоколы
noipv6
noipx
// IP-адрес локального хоста, выделяемый клиенту IP-адрес
192.168.1.41:192.168.1.51
// маска подсети
netmask 255.255.255.0
// IP-адрес нашего DNS-сервера
192.168.1.1
```

С помощью механизма sysctl включаем перенаправление IP-пакетов между сетевыми интерфейсами:

```
# sysctl -w net.ipv4.ip_forward=1
```

Добавляем диалапщика в систему, вводим и подтверждаем пароль:

```
# adduser -c "dialup user" -g users -s /usr/sbin/pppd dialer
# passwd dialer
```

И прописываем его вот в таком виде в базу PAP (двойные кавычки означают, что пасс берется из теневого файла паролей):

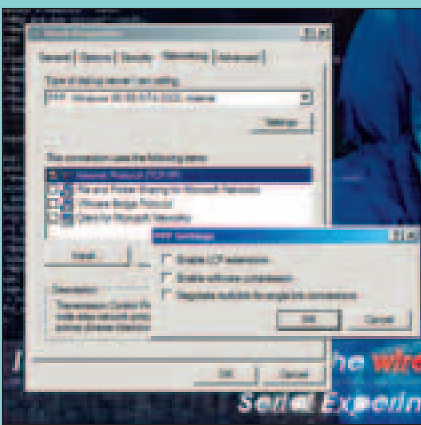
```
# vi /etc/ppp/pap-secrets

dialer     *     ""     *
```

Собственно, на этом настройка серверной части закончена, отдышавшись, перейдем к конфигурированию наших будущих кормильцев, то бишь клиентов-виндузятников :).

<КЛИЕНТСКИЕ ШТУЧКИ>

На стороне клиента у нас не будет никаких ухищрений и эксклюзивов: все абсолютно так же, как когда ты подключаешься к своему провайдеру. Создаем удаленное соединение, допустимые протоколы - только TCP/IP, тип dial-up сервера - PPP Windows 95/98/NT4/2000 Internet, IP-адрес и DNS сервера назначаются сервером, программное сжатие данных, номер телефона, имя и пароль.



Настраиваем клиента

<ПОСТСКРИПТУМНЫЕ ТИПСЫ И ТРИКСЫ>

Представленная конфигурация очень гибка и легко расширяема. Все зависит от твоих потребностей и фантазии. К примеру, ты можешь назначать как динамические, так и статические IP-адреса; выдавать шеллы; предоставлять доступ к расшаренным ресурсам локальной сети без доступа в инет (в файле /etc/ppp/options нужно убрать параметр proxyarp); создавать виртуальных диалапщиков без создания учетных записей в теневом файле паролей (следует убрать опцию login из /etc/ppp/options и добавить вручную имена пользователей и пароли в /etc/ppp/pap-secrets); разрешать модему отвечать на входящие звонки только в строго определенное время (пример см. во врезке 3) и многое другое.

На этом заканчиваю свой рассказ. Будут грабли - звони, т.е. пиши, адрес наверху.



По крону создаем пустой текстовый файл /etc/nologin.ttySX для того времени, когда наш модем должен молчать. Когда же он должен поднимать трубу, мы просто удаляем лочащий файл. В данном примере модем будет отвечать на входящие звонки с 9 вечера до 9 утра. Очень полезная фича :).

```
# vi /etc/crontab

0 9  * * 1-5 root  cp /dev/null /etc/nologin.ttyS0
0 21 * * 1-5 root  rm -f /etc/nologin.ttyS0
```

Взлом

ПОЧТОВЫЕ ШАЛОСТИ

CuTTer (cutter@real.xakep.ru)



Почтовые шалости

ИСПОЛЬЗУЕМ НЕДОРАБОТКИ SMTP ПРОТОКОЛА

Наверняка у тебя не раз появлялось желание отправить приятелю какое-нибудь гадостное письмо, но так, чтобы он не догадался о твоей причастности к этим проделкам. А может, тебя просто кто-то достал, и ты хочешь отомстить, отправив бесчисленное множество мусора во вражеский ящик. И опять же, мерзкий враг не должен знать, что это твоих рук дело. Что ж, это не проблема!

Не думай, что мы опять будем разбирать старые и замученные mail bomber'ы или почтовые веб-анонимайзеры. Нет, нет и еще раз нет! Это уже давно ушло в небытие, пользуется этим разве что сборище тупоголовой измороси. Ты ведь не причисляешь себя к этому многоумному сословию? Так что мы с тобой рассмотрим один забавный способ работы с SMTP протоколом, приводящий к неожиданным результатам. Поэтому активизируй свой мозг и читай дальше.

ПРОТОКОЛЫ, КОТОРЫМИ МЫ ПОЛЬЗУЕМСЯ

Как обычно, перед практикой немного поговорим о занудной теории. Ведь как устроена работа почтовой системы во всем интернете? Существует 3 базовых протокола: POP3, IMAP и SMTP (на самом деле их, конечно, больше, но остальные для нас неважны).

POP3 и IMAP отвечают за прием входящей почты. У них есть свои различия, например, IMAP поддерживает наличие папок, куда может складываться почта, POP3 же вываливает все в одну кучу. Каждый из них требует аутентификации по логину/паролю для чеканья почты. Причем, авторизацию можно проводить без какой-либо шифровки (открытым текстом, т.е. кто-нибудь может поснифать твой трафик, а оттуда вытянуть пароль от ящика), а можно и при помощи MD5 APOP (RFC-1734) или MD5 CRAM-HMAC (RFC-2095).

При работе с этими двумя протоколами удивляться не приходится - все работает нормально, просто проверяешь свой ящик, который защищен паролем. Но все становится гораздо интереснее, когда ты окунаешься в работу SMTP протокола...

НЕДОРАБОТКИ SMTP

SMTP протокол, в общем-то, прост. Он отвечает за пересылку писем от всяких там пользователей к нужному адресату. Как это происходит. Например, есть SMTP-сервер smtp.music.ru, он обслуживает пользователя jungle в домене music.ru. Т.е. мы имеем юзера с мыльником jungle@music.ru. И этот долбаный фанат Jungle и Drum'n'Bass культуры хочет, чтобы на диске Хакера выкладывали побольше музыки от LTJ Bukem'а и Omni Trio. Что же он делает? Берет и отправляет письмо на avalanche@real.xakep.ru с предложением выложить на компакт-диск этих музыкантов. Для пользователя jungle@music.ru вся эта процедура сложилась из открытия почтового клиента The Bat, создания письма и последующей отправки. А вот что было на самом деле. Когда он нажал на кнопку отправить, произошли следующие события:

Файл INFO.TXT

```
Received: from toghe.vseh.porot.ru by astral.ru
        via smtpd (for !smtp! [!smtpip!]) with ESMTP; Mon, 5 Aug 2003 23:20:57 +0400
Received: from porol.v.rot.ru by toghe.vseh.porot.ru
        via smtpd (for astral.ru [10.128.2.21]) with ESMTP; Mon, 5 Aug 2003 23:20:45 +0400
Received: from scuka.loh.ubogiy.ru ([213.1.2.3]) by porol.v.rot.ru
        via smtpd (for toghe.vseh.porot.ru [192.168.0.3]) with ESMTP; Mon, 5 Aug 2003
23:18:57 +0400
```

1) Клиент соединился с SMTP-сервером smtp.music.ru. Возможно, была проведена SMTP-аутентификация, это уже зависит от конкретных настроек сервера. Далее пользователь передал письмо серверу, получил в ответ, что все ок. Отсоединился.

2) Теперь в работу вступил сервер smtp.music.ru. Из письма он получил конечный пункт назначения - avalanche@real.xakep.ru. Вот что происходит потом. SMTP-сервер делает DNS-запрос по домену real.xakep.ru. Из него он вытягивает MX запись. В ней содержится адрес другого SMTP-сервера, отвечающего за домен real.xakep.ru - smtp.gameland.ru. Он соединяется с smtp.gameland.ru и передает ему письмо пользователя, добавив в него служебную информацию об IP'шниках.

3) Это письмо получает SMTP-сервер smtp.gameland.ru. Он смотрит свою таблицу маршрутизации и видит, что avalanche@real.xakep.ru - его ящик. Поэтому smtp.gameland.ru принимает письмо и кладет его в базу. Теперь пользователь avalanche может забрать новую почту по POP3 протоколу.

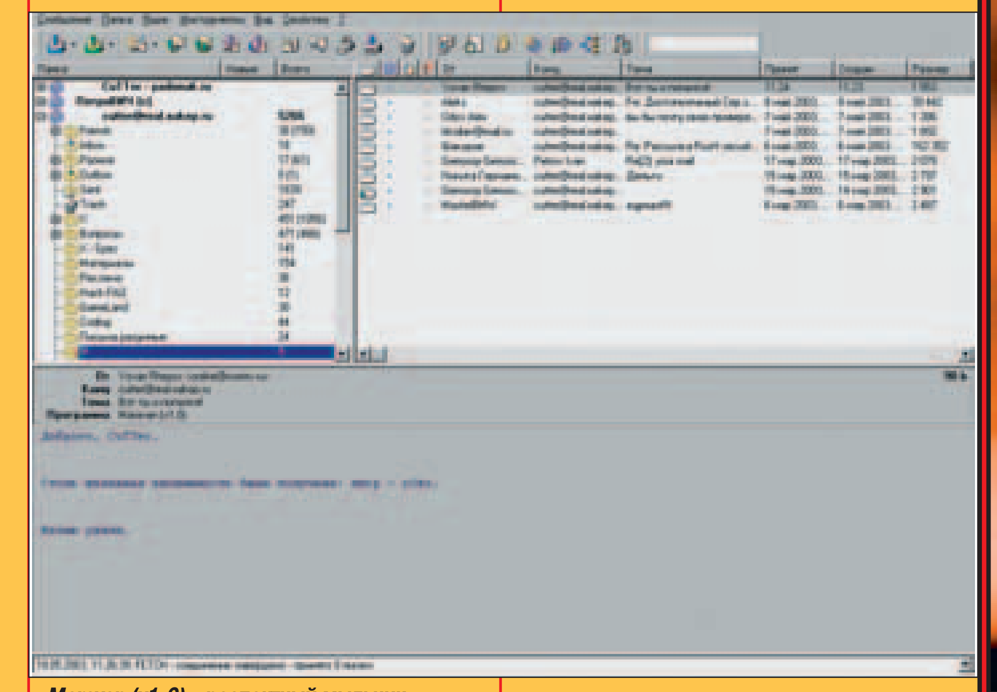
Как видишь, схема работы SMTP протокола проста. Ты отправляешь письмо своему SMTP-серверу, а дальше все заботы об отправке он берет на себя. Сама цепочка, по которой проходит письмо, может состоять из одного сервера, а может и из десятка. Все зависит от настроек сервера, а именно от таблицы маршрутизации. Например, если ты пошлешь письмо с почтового ящика vasya@comtv.ru на anya@comtv.ru, то цепочка SMTP-серверов будет состоять всего из одного сервера. Но в случае, когда письмо будет предназначено для anya@mail.ru, количество SMTP-серверов, участвующих в пересылке письма, заметно возрастет.

ИДЕЯ ОБМАНА

Ты можешь возмутиться, мол, зачем мне нужна вся эта теория? А она, поверь, нужна... Если ты внимательно прочитал второй пункт, то должен был заметить, что в само письмо добавляется информация о том, с какого IP отослано письмо, а также IP-адреса серверов, отвечавших за пересылку письма. По этой инфе как раз и можно восстановить всю цепочку SMTP-серверов.

Мы же, наоборот, эту цепочку будем корректировать, а попросту говоря, возьмем да и запишем в нее всякий мусор. Так что конечному адресату, если ему вдруг захочется заглянуть в заголовки письма, останется только ужасаться, почему же это письмо идет по цепочке: gryaznhaya.shlyuha.ru (1.1.1.1), moya.volosotaya.grud.ru (10.0.0.10), zlya.golubaya.mraz.ru (217.10.10.43). При виде такого приходишь к выводу - письмо шло тернистым путем.

Для реализации этого обмана нам придется выступить в роли псевдо SMTP-сервера. Этот сервер будет принимать письмо, резать всю предыдущую инфу, а потом посылать письмо дальше настоящему SMTP-серверу. Причем, наш почтовик будет работать абсолютно прозрачно, т.е. для отсылки письма не понадобятся какие-то дополнительные извращения. Потребуется только установить наш хитрый SMTP-сервер и проставить его в настройках почтового клиента (SMTP настройки).



Maravan (v1.0) - респектный мыльник

КОДИНГ

Как принято, всю эту бойду я реализовал на перле :). Основная часть кода состоит из обычного редиректа пакетов при TCP соединении. Если тебе интересно в этом разобраться, возьми старый номер][05.01 и открой статью "Дело - труба! Datapipe roxx" или почитай на нашем сайте по адресу http://www.xakep.ru/magazine/xa/029/068/1.asp.

В общем, я взял и переделал файл datapipe.pl. Добавленный код смотри во врезке на следующей странице.

Тебе стоит поменять в нем только следующие переменные:

$localport - порт, на котором будет работать наш SMTP-сервер. Если будешь пускать локально со своей тачки, то можешь оставить и его (25). Если же это *nix тачка, где у тебя отсутствуют root права, то поставь любой порт выше 1024.

$host - хост настоящего SMTP-сервера. Именно на него будет пересылаться скорректированное письмо. Также с ним будет происходить SMTP аутентификация, если она нужна.

$port - номер порта настоящего SMTP-сервера. Обычно всегда равно 25.

$name - приветствие при соединении. Отправляется в команде HELO. Можешь поменять на что-нибудь свое.

$mailer - имя почтовика. Добавил для розыгрыша "умных" людей. Например, можешь написать туда, что у тебя "The Bat! (v2.03) Personal" или "Zlobodrom (v1.0)". Теперь у получателя письма в заголовках будет отображаться не какой-нибудь Outlook Express, а что-то более продвинутое.

$log - логирование. 0 - выключено, 1 - включено. На самом деле можешь не включать, оно тебе на фиг не нужно.

Осталось создать еще один файл info.txt. В нем как раз и находится цепочка левых серверов, которая добавится в письмо:



Взлом

ПОЧТОВЫЕ ШАЛОСТИ

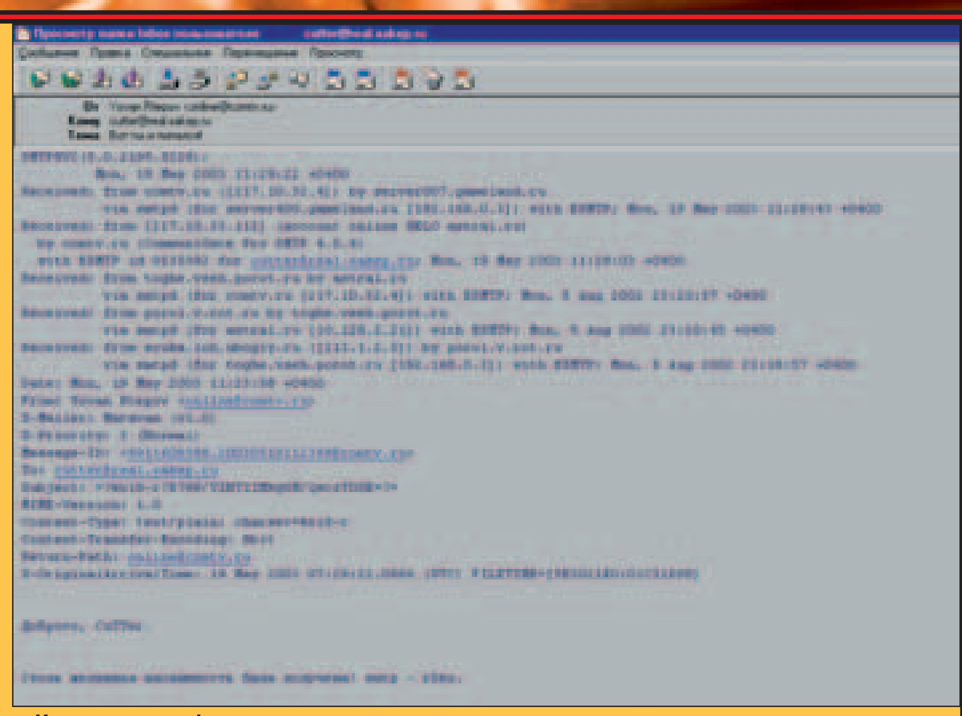
CuTTer (cutter@real.xakep.ru)

Этот файл можешь менять как угодно. Все зависит от твоей фантазии и извращенности. Единственное, на что необходимо обратить внимание, это две записи: !smtp! и !smtpip!. Их придется оставить, чтобы не ломалась "правдивость" письма. Иначе пользователь сразу заметит, что цепочка рвется, причем самым наглым образом.

УСТАНОВКА

Здесь все просто. Для начала скачиваешь архив mailjoke.zip с www.xakep.ru (смотри раздел X-Релизы) или берешь его с нашего диска. Далее распаковываешь это добро и делаешь необходимые корректировки в описанных выше переменных. Заливаешь файлы, причем желательно на какой-нибудь *nix сервер. Проставляешь права 755 файлу mailjoke.pl (chmod +x mailjoke.pl). Все, наш SMTP-сервер готов к запуску - ./mailjoke.pl. Сервер заработал.

Открывай почтовик. Поставь в настройках адрес нашего нового SMTP-сервера. Допустим, это maravan.ru:1025. Теперь для проверки напиши любое письмо самому себе. Отправь и чекни свою почту. Открой новое письмо. Обрати там внимание на имя почтовика и на саму цепочку адресов (для этого включи отображение служебной информации). У тебя должно получиться что-то типа этого:



Извращенная инфа в почтовике

Получилось весьма забавно :). Теперь, помимо шуток над своими друзьями, ты получил и анонимность в отправке писем. Так что совместили приятное с полезным.

ЧЕГО ЖЕ НЕ ХВАТАЕТ?

Естественно, наша программа несовершенна. Она, например, всегда отправляет дурацкие даты в письме. У пользователя при просмотре это вызовет как минимум недоумение, а если задуматься глубже, то станет ясно, что письмо - fake. Поэтому даты надо подставлять уже во время отправки письма, а не хранить готовыми в файле. Также стоит добавить генератор различной длины цепочек. Причем, генерировать их с разными баннерами (т.е. менять via smtpd with ESMTP на что-то другое), подставлять живые хосты, чтобы у пользователя не возникало лишних подозрений. Можно создать массив значений для поля X-Mailer. Тогда получатели писем будут удивляться, что же это за отправитель такой странный. В общем, идей можно позапихивать предостаточно. Главное - выделить под это свое время.

Так что дерзай! И оставайся для всех анонимным. Ибо нечего выдавать себя :).

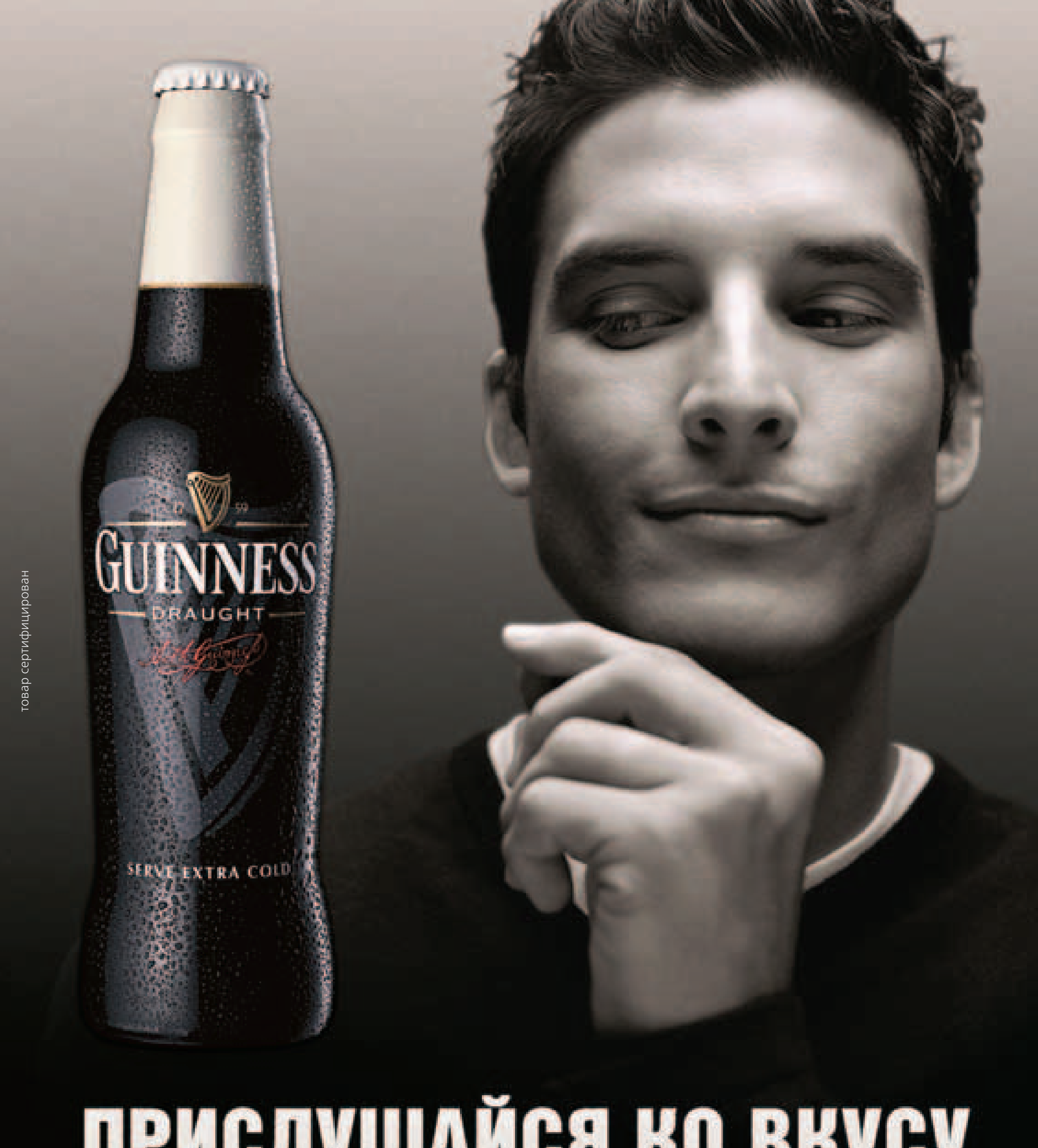


Код, отвечающий за переделку письма

```
$localport=25; # SMTP
$host="comtv.ru"; # SMTP server
$port=25; # port of SMTP server
$name="astral.ru"; # name in HELO/EHLO
$mailer="Maravan (v1.0)";
$log=0;

## Skipped some code

## Добавление левой инфы в письмо
if (($info{helo}==0) && ($tbuffer=~/^HELO /i)){
        $tbuffer="HELO $name\n";
        $info{helo}=1;
}
if (($info{helo}==0) && ($tbuffer=~/^EHLO /i)){
        $tbuffer="EHLO $name\n";
        $info{helo}=1;
}
## Смена X-Mailer
if (($info{mailer}==0) && ($tbuffer=~/X-Mailer: .*\r?\n/i)){
        $tbuffer=~s/X-Mailer: .*\r?\n/X-Mailer: $mailer\n/i;
        $info{mailer}=1;
}
## Изменение хедера письма
if (($info{server}==0) && ($tbuffer=~/Date: /i)){
        $tbuffer=$info.$tbuffer;
        $info{server}=1;
}
```



ПРИСЛУШАЙСЯ КО ВКУСУ GUINNESS DRAUGHT

Так бьется сердце Guinness. В каждую бутылку мы поместили специальную капсулу, которая и создает знаменитую бархатную пену. Так Guinness становится Draught. Теперь ты можешь наслаждаться легендарным ирландским пивом Guinness Draught не только в баре.

Guinness Draught. Отныне повсюду

Докучаев Дмитрий aka Forb (forb@real.xakep.ru)

ОБЗОР ЭКСПЛОИТОВ

BYSIN2 EXPLOIT FOR SENDMAIL

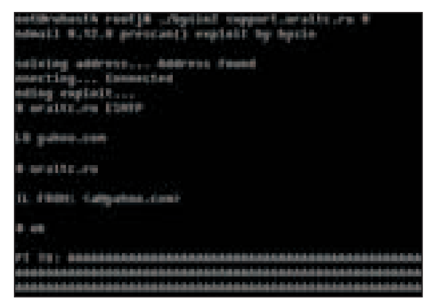
Описание:
Совсем недавно во всех багтраках пролетело долгожданное известие о выходе эксплоита для Sendmail <= v.8.12.8. Этот экземпляр является типом Proof of Concept (POC), то бишь бесполезной вещью в руках скрипткидди. Эксплоит только показывает, что Sendmail действительно уязвим и падает в кору при передаче ему смертельного кода. После удаленных экзекуций над сендмылом и последующего анализа core-файла, можно увидеть запись:
Program received signal SIGSEGV, Segmentation fault.
0x5c5c5c5c in ?? ()
В эксплоит вшит один-единственный таргет: FreeBSD 4.7. Но, как ты понимаешь, Бздюх с непропатченными сендмылами в инете пруд пруди, ибо FreeBSD 4.7 до сих пор остается самой надежной системой.

Защита:
Пока это POC эксплоит. Но это только начало. Совсем скоро можно ожидать выхода нового сплоита для Sendmail, которым смогут воспользоваться и скрипткиддисы. Так что настоятельно рекомендую всем админам обновить версию сендмыла.

Ссылки:
Эксплоит, демонстрирующий уязвимость почтового сервера, ты можешь скачать по адресу: http://packetstormsecurity.nl/0304-exploits/bysin2.c.

Злоключение:
Я сомневаюсь, что все будут рыться в чужом коде, чтобы довести его до боевого состояния. Проще подождать, пока за тебя это сделают более умные люди. И возможно, через месяц-другой ты увидишь byson3.c, который уже реально порутает сервак. Но если ты нетерпелив - бери gdb в руки и пусть тебе улыбнется удача! :)

Greets:
В архивы эксплоит был выложен неким Bysin. Человек это или название хак-группы - одному Богу известно.



Эксплоит в действии

0X333HATE EXPLOIT FOR SAMBA 2.2.X

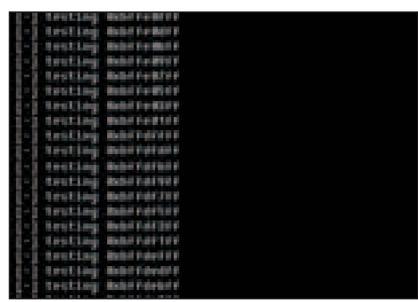
Описание:
В этом месяце вышел еще один удаленный эксплоит для Самбы. Как видно из кода, он использует ошибки в переполнении буфера (как и все его предшественники). Судя по высказываниям разработчиков, эксплоит базируется на trans2root.pl - зло-скрипте, который кладет непропатченные smbd. По утверждению авторов, в случае успеха программа предоставит хакеру рутшелл. Но за две бессонные ночи, проведенные в поисках жертвы с уязвимой самбой, мне не удалось порутать ни один сервер. Кто знает, может фортуна отвернулась от меня, либо авторы внесли защиту от дурака в свой код...

Защита:
Защититься от злоумышленника тебе поможет только апдейт. Если у тебя до сих пор стоит smbd v. <=2.2.x, немедленно обновляй свой софт, иначе потом будет поздно.

Ссылки:
http://packetstormsecurity.nl/0304-exploits/0x333hate.c - рабочая версия эксплоита для Smbd v.2.2.x.

Злоключение:
Как я уже сказал, мне не удалось найти жертву с непропатченной самбой. Но это не повод для отчаяния. Инет огромен, и жертв в нем всегда много. Как говорится - кто ищет, тот всегда найдет.

Greets:
Дружно снимаем шапки перед хакерской командой 0x333. Эксплоит был выложен мембером c0wboy. Если тебя интересуют другие творения этой тимы - добро пожаловать на www.0x333.org.



Долгий брутфорс адреса...

OPENFUCKV2 EXPLOIT FOR OPENSSL V0.9.6D

Описание:
Еще совсем недавно была актуальна уязвимость в OpenSSL, для которой моментально появился рабочий эксплоит под устрашающим именем OpenFuck :). Только в этом месяце вышла вторая версия эксплоита.
Такого количества таргетов я не видел нигде. Если в первой версии было около 20-30 рабочих целей, то во второй их уже 138. Тут и RedHat, и Mandrake, и Cobalt, и даже FreeBSD.
Используя ошибку в протоколе SSL, эксплоит переполняет буфер и запускает интерактивный шелл с правами nobody (в Cobalt даже с правами root!), предоставляя тебе возможность "добить" жертву локально (при помощи того же ptrace-kmod exploit, про него говорилось в предыдущем обзоре).
Авторы эксплоита позволяют добавлять свои цели. Для этого надо узнать адрес переполнения и изменить константу MAX_ARCH в теле эксплоита. По умолчанию она равна 138.

Защита:
Большинству админов хватило первой версии, чтобы побороть собственную лень и обновить-таки апач и OpenSSL до более свежих версий. Но существуют люди и с иным мнением :). Надеюсь, ты не в их числе. Так что на всякий случай проверь, чтобы версии твоего апача не было в таргетах этого чудо-эксплоита.

Ссылки:
Скачать вторую версию OpenFuck можно по адресу: http://packetstormsecurity.nl/0304-exploits/OpenFuckV2.c. Обязательно используй ключик -lcrypto для компиляции эксплоита.

Злоключение:
Вторая версия дает лишь разнообразие целей. Но помни, что админы давно уже пропатчили свои системы, ибо столкнулись с толпой скрипткиддисов, атакующих их сервера :). Но чем черт не шутит, если в инете еще полно непропатченных IIS серверов, то дырявых OpenSSL должно быть еще больше... Поиск, поиск и еще раз поиск!

Greets:
Эксплоит был выложен в public-архивы неким Spabam. Сайт автора http://spabam.tk. Для тех, кто желает пообщаться с ним вживую, рекомендую зайти на IRC-канал #hackarena сервера irc.brasnet.org, предварительно захватив с собой русско-бразильский словарь :).

138 таргетов в твоем распоряжении! =)

Юниксоид

ИНТЕРВЬЮ С ДЖОНАТАНОМ КОРБЕТОМ

TanaT (TanaT@hotmail.ru)



Полет на ядре

Интервью с Джонатаном Корбетом

Джонатан Корбет (Jonathan Corbet) написал книгу по ядру Linux (сейчас работает над ее третьим изданием) и создал Linux Weekly News, исполнительным редактором которого он сейчас и является. В этом интервью Джонатан раскрывает основные концепции ядра UNIX и объясняет свой интерес к этой теме.

X: Джонатан, можете объяснить, почему вас привлекает именно ядро операционной системы?

JC: Хороший вопрос. Впервые я серьезно заинтересовался операционными системами в 1980 году (ну, примерно), когда Эва Немес (Evi Nemeth) разрешила мне повозиться с VM-алгоритмом в ранних версиях BSD для VAX 11/780 (Virtual Address eXtension – популярное семейство 32-разрядных миникомпьютеров, выпускавшихся с 1978 по 1990 г. бывшей корпорацией Digital Equipment Corp. - прим. автора). Программирование на уровне ядра – это своего рода соревнование: вам всегда приходится думать о том, что может произойти в другом месте системы, там, где вы этого не ожидаете. Если программист ядра все сделал правильно, система правильно работает во всех ситуациях. Правда нужно заметить, что низкоуровневый программист не может отвечать за более высокие системные слои. Я всегда интересуюсь тем, что происходит за сценой. К примеру, если я веду своих детей в цирк, то обращаю больше внимания не на представление, а на людей «в черном», которые помогают актерам исполнять свои номера. Та часть жизни, которая скрыта от глаз, наиболее интересна.

X: А кто такая Эва Немес?

JC: О, Эва – это человек, хорошо известный в кругу BSD и USENIX сообществ. Она является профессором (в отставке) Колорадского Университета (University of Colorado). Она также соавтор книги «Unix System Administration Handbook» (позднее она была переработана в Linux System Administration Handbook).

X: Что такое VM-алгоритм? Очень похоже на виртуальную память.

JC: Да, так и есть. Давным-давно, в 1981 году, 4BSD, использующая виртуальную память, была еще очень молодой системой. Эва испытывала затруднения с большими приложениями. Когда те загружались в память, все остальное приходилось принудительно сбрасывать в swap. Естественно, при этом страдала производительность – система реагировала на события слишком медленно. Не забывайте, что в те времена использовались VAX 11/780. Когда к ним подключалось большое число пользователей, медленная реакция доводила людей до истерики. Я усовершенствовал алгоритм сканирования страниц памяти таким образом, чтобы записывать в swap лишь информацию,



принадлежащую ресурсоемким процессам, а все остальное оставлять в памяти. Это было мальчишеским баловством, и, конечно же, ни у кого не возникло желания послать мой код в Беркли для рассмотрения его экспертами. Однако именно этот опыт положил начало моим исследованиям ядра.

X: Опишите, пожалуйста, структуру ядра Linux.

JC: Это довольно сложный вопрос, но я все-таки попытаюсь ответить. Ядро Linux является монолитным, то есть отдельным, большим образом, который содержит в себе все основные системные функции. В этом смысле такое ядро отличается от ядер таких систем, как Mach (которые основаны на небольших ядрах с прохождением сообщений). Ядро можно разделить на подсистемы: виртуальную память, файловую систему, сетевую поддержку и т.д. Как и большинство ядер, ядро Linux - большая программа, реагирующая на события. Большую часть времени (в идеале) ядро ничего не делает. Оно спокойно посапывает и не мешает пользователю работать со своими приложениями. Как только что-то требует внимания ядра (например, аппаратное прерывание, системный вызов, создающий процесс), ядро реагирует на событие и выполняет требуемые действия. Затем оно снова возвращает контроль приложениям пользователя.

X: Вы не могли бы подробнее пояснить суть термина «монолитное ядро»?

JC: Это довольно просто. Монолитное ядро – это больший цельный «кусок». При этом существует всего один исполняемый образ и одна большая непрерывная часть памяти, где данный образ хранится. Все привилегированные операции (доступ к аппаратному обеспечению) проходят через образ ядра. В противоположность монолитным существуют микроядра. Микроядра строятся на минимуме требуемой функциональности: механизме прохождения сообщений и контроле над процессами. Все остальные функции берут на себя привилегированные внешние процессы. Таким образом, поддержка сетей, файловой системы и аппаратных драйверов вынесена из ядра и размещена во внешнем коде.

X: В чем на практике проявляется разница между такими подходами к строению ядра?

JC: Микроядра долгое время претендовали на первое место, но судьба решила по-иному. Микроядра обещали и производительность, и переносимость, и практическую гибкость. Когда система собирается из маленьких кусочков (составных частей ядра), вы можете многое поменять, модифицировав лишь требуемый кусочек. Когда дело дошло до практики, микроядра не оправдали ожиданий. «Микро»-часть ядра на деле является не такой уж и маленькой, а добиться нормального уровня производительности оказалось не так просто. Высокая скорость легко достигается, если ядру не требуется обрабатывать большое число сообщений и переключать контекст для каждой операции. Те, кто действительно интересуется этой темой, могут просмотреть знаменитый спор между Линусом Торвальдсом и Эндрю Танненбаумом (Linus Torvalds и Andrew Tannenbaum): www.oreilly.com/catalog/opensources/book/appa.html.

X: Можете привести примеры операционных систем, построенных на микроядрах?

JC: Windows 2000 построена на микроядре. Пожалуй, больше я и не знаю :). В мире свободного ПО Mach является известной системой на архитектуре микроядра. Это ядро положено в основу Apples OS X, а также используется в проекте GNU HURD.

X: Расскажите, пожалуйста, об ошибках и багах, содержащихся в коде ядра.

JC: Огромное количество багов живет в коде годами. И никто их не замечает. Проект Stanford Checker предлагает некоторые средства, позволяющие автоматизировать процесс поиска багов. Хотя большинство багов безобидны, некоторые из них все же могут вызвать серьезные проблемы. Переполнение буфера и тому подобное встречается в ядре довольно редко. Разработчики ядра очень внимательно относятся к таким вещам и делают все возможные и невозможные проверки, чтобы предотвратить любые переполнения. Настоящие проблемы вызывают баги, связанные с аппаратным обеспечением и параллельной обработкой. Очень сложно поддерживать аппаратное обеспечение, которое только появилось на складах магазинов, но которое вот-вот уже установит себе пользователь. К тому же производители железа не всегда следуют предписанным спецификациям и допускают некоторые отклонения. Основная причина необходимости в огромном числе тестеров в том, что у разработчиков просто не может быть всех возможных видов аппаратного обеспечения. Пользователи же легко наткнутся на проблему, когда какая-то определенная сетевая карта или, к примеру, новый дисковод ведут себя немного по-другому. Но этого хватит, чтобы повесить систему. Параллелизм связан с тем, что в ядре многие события происходят одновременно. Вы можете запрограммировать простое выражение вида:

a = a + 1;

Компьютер же воспримет его в следующем виде:

- считать значение переменной «a»;
- прибавить к нему 1;
- сохранить результат обратно в «a».

Но на практике возможно, что какой-то другой поток ядра изменит значение «a» между первым и третьим шагами. Избежать этой «гонки» (такое название потому, что результат зависит от того, кто первый сохранит свое значение в «a») и есть главная задача программиста ядра.

X: Какие виды исключительных ситуаций могут возникнуть при работе ядра?

JC: Ядро Linux имеет два вида исключений, называемых обычно «oops» и «panic». Как и с каждой системой, паника происходит тогда, когда ядро обнаруживает серьезную неисправность. Если система каким-либо образом повредила сама себя, ей требуется немедленно остановиться, пока она не сделает что-нибудь типа уничтожения файловой системы. Везде, где только возможно, Linux пытается детектировать проблему и справиться с ней без остановки всей системы. Например, многие ситуации типа «oops» приводят к завершению процесса, который нормально запустился, но потом зациклил систему. Но бывают ситуации, когда все настолько плохо, что полная паника является наилучшим выходом. Пользователи стабильных версий ядра, конечно же, никогда не видели ни паник, ни «oops». Но в реальном мире они иногда происходят.

X: Можете привести больше примеров ситуаций, когда возникают паника или «oops»?

JC: Недавно найденный TF баг (смотрите http://lwn.net/Articles/15903/) служит хорошим примером паники. Процессор пытается передать управление процессу, которого не существует. Это приводит к краху всей системы. В данном случае у системы нет другой альтернативы, кроме как паниковать. Ядро, поставляемое с Red Hat Linux 7.3 (и некоторыми другими дистрибутивами) содержит баг в файловой системе ext3. Эта ошибка приводит к «oops», завершая время от времени некоторые процессы. К тому же этот баг приводит к замедлению всей системы. Хотя данная ошибка уже исправлена (патч есть и в обновлении от Red Hat), этот случай познакомил многих пользователей с ошибками типа «oops».

X: Какие функции выполняет ядро Linux?

JC: Ядро делает все то, что не может быть выполнено в пространстве пользователя. Это означает контроль над доступом к ресурсам: ядру, файловой системе, устройствам и т.д. Некоторые задачи, которые могут быть выполнены на более высоком уровне, вынесены в ядро для увеличения производительности. Например, сетевое взаимодействие. Иногда пользователи сами добавляют некоторые функции в ядро по той же причине. Например, сетевой сервер TUX (доступен как отдельный пакет) предоставляет сетевые услуги прямо на уровне ядра (с впечатляющей скоростью, надо сказать). Критерием яв-

NEXT

Юниксоид

ИНТЕРВЬЮ С ДЖОНАТАНОМ КОРБЕТОМ

TanaT (TanaT@hotmail.ru)



ляется интерфейс системных вызовов: пользовательский уровень и ядро общаются между собой вызовами типа open() (функция служит для открытия файла и доступа к данным), fork() (основная функция API процессов, используется для создания нового процесса) и т.п.

X: То есть ядро контролирует работу файловой системы?

JC: Да. Хотя возможно реализовать файловую систему на более высоком уровне, этого никто не делает. Опять же из соображений производительности. Скорость файловой системы составляет скорость всей системы в целом. Поэтому поддержка файловых систем, которыми пользуются наиболее часто, включена в ядро.

X: Считается, что ядро Linux не содержит никаких решений для ускорения работы графических сред. Конечно, оболочек для Linux довольно много. Но сегодня можно выделить сверхпопулярные GNOME и KDE. Почему не включить в ядро Linux поддержку этих графических сред? Для увеличения производительности. Почему третьи лица не выпускают ядра с поддержкой графических оболочек?

JC: Ну, например, ядро 2.5 имеет встроенный слой буфера кадров. Он используется для доступа к видеоустройствам. Хотя не ясно, насколько эффективен данный метод, ведь и X-сервер предоставляет хороший низкоуровневый доступ к видеоустройствам. Перенос X-сервера в ядро увеличил бы его до гигантских размеров. Это также означало бы, что любые ошибки и проблемы безопасности в X-сервере (это довольно большое приложение само по себе) могут с легкостью положить на лопатки всю систему. К тому же выгоды от такого переноса не очень ясны. Поэтому никто и не хочет так делать. Если говорить о GNOME и KDE, то они являются приложениями более высокого уровня, чем X-сервер. Поэтому у них еще меньше причин попасть на уровень ядра.

X: Возвращаясь к файловой системе: зачем Linux поддерживает несколько разделов? Windows, к примеру, использует один большой NTFS или FAT32 раздел, а Linux минимум два: Linux native и swap. Чем это обусловлено?

JC: Linux может работать и без swap, а Windows может использовать swap. Здесь нет никакого различия. Swap это лишь способ расширить оперативную память. Инсталляция Linux может разбить файловую систему на несколько разделов (а может и не разбивать). Существует несколько причин, почему следует так сделать:
- Если в одном разделе не хватит места, это никак не отразится на остальных;
- Если каким-либо образом один раздел будет поврежден, другие останутся целыми;
- Вы можете использовать разные файловые системы в разных разделах. Например, ext3 для основной файловой системы, XFS для раздела, содержащего огромные научные базы данных.
- И, конечно же, если у вас несколько дисков, то обойтись одним разделом точно не удастся. Хотя есть способы, как это спрятать.
Linux может работать и на одном большом разделе.

X: Что вы можете сказать о стабильности файловой системы Linux? Экспериментально установлено, что компьютер с Windows XP + NTFS можно включать/выключать несколько раз подряд (я видел раз 15-20) и при этом не будет никаких ошибок в файловой системе (NTFS). Linux может похвастаться такими же результатами?

JC: Я не могу определить, какая файловая система стабильнее. Я могу лишь сказать, что более чем за 10 лет использования Linux единственная проблема с файловой системой, которая у меня была, случилась, когда я установил нестабильное «горячее» ядро.

X: Чем отличаются ядра Linux и BSD систем?

JC: Прошло много времени с тех пор, как я интересовался ядром BSD, так что не уверен, что смогу ответить точно. Корни ядра BSD намного старше и более распространены, чем Linux'a. Реализация TCP/IP в современной BSD сохранила немало общего со своими самыми старыми версиями. Что же до Linux, то он с самого начала был построен по-другому, в частности Linux использует свой собственный сетевой стек. Конечно, системы немало повлияли друг на друга за последние годы. Одна из самых приятных черт свободного ПО это то, что хорошие идеи очень быстро распространяются и внедряются. К примеру, хотя Linux имеет собственную реализацию виртуальной памяти, он позаимствовал немало мудрых решений из VM-кода FreeBSD.

X: А вы отвечаете за какую-нибудь конкретную часть ядра?

JC: Нет, я не вхожу в команду, которая поддерживает какую-либо часть ядра и отвечает за нее. У меня никогда не хватало на это времени, хотя было бы интересно попробовать. Я часто выпускаю небольшие патчи для ядра, которые исправляют ту или иную проблему. Мой самый значительный вклад в разработку ядра это второе издание Драйверов Устройств для Linux (Linux Device Drivers) в соавторстве с Алессандро Рубини (Alessandro Rubini). LDD было выпущено под лицензией Free Documentation License.

X: В состоянии ли один человек написать ядро? Какие знания для этого требуются?

JC: Ну, Линус доказал, что это возможно. Понимаете, не так уж и сложно написать ядро, которое сможет обрабатывать основные системные вызовы, управлять процессами и устройствами и т.д. А вот создать ядро, которое принесет что-то полезное в этот мир, задача намного более сложная. Ядро Linux не является работой какого-то отдельного разработчика, это результат работы сотен программистов по всему миру. Что касается знаний и навыков, то необходимо владеть языком программирования, обеспечивающим низкоуровневый доступ к внутренностям машины. Именно поэтому ядро Linux написано на C и (небольшая часть) на ассемблере. Много лет назад была идея переписать ядро Linux на C++, но ее забросили. Среди прочих вещей, C++ скрывает некоторые вещи, происходящие в глубине. Это сильно снижает контроль и производительность, что не позволяет выполнять требуемые задачи.

X: То есть нужно хорошо разбираться в C и ассемблере, так?

JC: Если вы хотите написать свое собственное ядро, вам, конечно же, понадобится ассемблер для работы с процессором, под который вы программируете. И язык более высокого уровня (например, C). Многие люди, занимающиеся ядром Linux, не особо разбираются в ассемблере, им вполне хватает и C.

X: Почему ядро Linux так часто обновляется?

JC: «Выпускайте как можно раньше, обновляйте как можно чаще» - это девиз разработки свободного ПО. Часто выпуская новые версии, Линус позволил другим разработчикам (и пользователям) следить за всем, что происходит и, я надеюсь, отслеживать любые проблемы на самой ранней стадии. На самом деле пользователи Linux обновляют ядро не так уж и часто. Существуют стабильные реализации ядра – они появляются раз в два года. Все остальные обновления направлены лишь на устранение найденных ошибок.

X: Есть ли смысл в обновлении своего ядра Linux? Не лучше ли установить какую-нибудь стабильную версию и оставить свою систему в покое?



JC: В общем случае, если система вас полностью устраивает, не следует в ней что-либо менять. Кроме тех случаев, когда новое ядро позволяет делать что-то очень вам нужное, обновление ядра того не стоит. Ну, а если говорить о «горячих» версиях (типа 2.5.x), то, устанавливая их, вы должны быть готовы столкнуться с потенциальными проблемами. Многие любят быть «впереди планеты всей», для них это достаточное основание для обновления ядра.

X: Что вы можете сказать об оптимизации ядра? Если говорить о домашних пользователях, которым не нужно, чтобы ядро поддерживало все виды устройств. Имеет ли смысл им оптимизировать ядро?

JC: Это зависит от рода деятельности этих людей. Ядро 2.6 содержит много изменений, уменьшающих латентность (максимальное время, которое требуется ядру, чтобы среагировать на событие). Низкая латентность очень важна для некоторых видов приложений, например, для потокового видео и аудио. Пользователи, которым важны эти области, следует обновить свое ядро до одного из самых последних. Если вы спрашиваете о возможности создать свое собственное ядро, которое будет приспособлено к конкретным нуждам, то, хотя многие пользователи и хотят это сделать, это нерационально. Большая часть дистрибутивов Linux использует высокомодульные ядра. Это приводит к тому, что неиспользуемые возможности (файловые системы, устройства, которых нет на данной машине и т.д.) не грузятся в память.

X: Вы знакомы с новым средством разработки Borland Kylix? Как он вам?

JC: Я не думаю, что многие разработчики ядра знакомы с ним. Мы чаще всего ограничиваемся свободными инструментами. Хотя я и видел Kylix, много о нем сказать не могу. По-моему, очень хорошее средство для программирования ядра - User-mode Linux (user-mode-linux.sourceforge.net). Используя UML, вы можете запустить копию ядра как обычный процесс Linux. Это значит, что любые сбои и ошибки не приведут к краху всей системы. К тому же вы можете использовать обычные инструменты отладки.

X: Расскажите о своих личных предпочтениях в Linux.

JC: Я работаю с несколькими дистрибутивами. Чаще всего приходится использовать нестабильный Debian. Нестабильная версия позволяет с легкостью устанавливать любые пакеты, управлять ими и не обращать внимания на такие вещи, как зависимость пакетов друг от друга. В качестве графической среды я использую GNOME. В основном потому, что я начал с него и привык. Если GNOME исчезнет завтра, я не сильно расстроюсь и перейду на KDE. Единственное, чему всегда удивляются люди, так это тому, что я люблю пользоваться и emacs и vi. Серьезным программированием я занимаюсь в emacs, но ничего не может быть лучше vi, если надо быстро что-то сделать. Так что я часто запускаю emacs для себя и vi как root.

X: Хотите сказать что-нибудь нашим читателям?

JC: Свободное ПО – это великая вещь. Но оно сильно зависит от свободы того общества, в котором разрабатывается и используется. Сейчас многие ратуют за «интеллектуальную собственность» и ее изъятие из общего пользования. Linux, как и множество других вещей, зависит от существования свободного интеллектуального общества. Именно там он черпает свои идеи. Те, кто использует Linux и другие свободные продукты, должны знать, что им придется бороться и защищать свободное ПО.



Лозовский Александр (klouniz@mail.ru)

Свой ZIP на Delphi.

Быстро, качественно, недорого!

После выхода в свет Delphi 2 количество компонентов, содержащих функции разных архиваторов, стало увеличиваться в геометрической прогрессии. Уж не знаю, зачем это надо, но разнообразие стало пугающим: размер их варьировался в пределах от 30 Кб до 2 Мб, цена - от 0 до 299 долларов, а функций… В общем, очень много. До Delphi 4 эти компоненты постепенно прогрессировали и пополнялись новыми фичами, но вот потом наступил резкий спад. До 6 версии дожили, по моим подсчетам, около 4-5 достойных представителей. Это действительно монстры. Правда, XEEDZIP, который теперь весит 16 Мб, я так и не рискнул скачать, но в целом это функциональные и дорогие продукты, вполне достойные такого нищего кодера, как я :).

Лозовский Александр (klouniz@mail.ru)

Сегодня мы будем пользоваться компонентом (вернее, целой коллекцией компонентов) под названием ZipTV. Я выбрал его потому, что там есть все, что нужно для работы с архивами. Он сравнительно мало весит и не содержит ничего лишнего. Зато есть кое-что и для настоящего][. В конце концов, в нем отлично сочетаются простота и функциональность - научиться его использовать проще, чем двигать черепашку в LogoWr, а написать с его помощью WinZip - дело 10 минут. Нужно только немного мозгов, ловкость рук и никакого мошенничества.

Реквизит

Можешь забрать его с http://www.ziptv.com/download/ZipTV_u6_5.3.0.exe (он весит 2.08 Мб) или заглянуть на наш диск. Там в качестве бонуса мы положили тебе еще несколько компонентов. Так сказать, для домашнего изучения. Инсталляция его проходит безо всяких проблем. Главное - ставить его в пустую директорию (во избежание жертв), а после установки убедиться (посмотрев в tools-> environment options-> вкладка library) в том, что путь к этой самой директории там прописан. Иначе потом придется выяснять, почему компонент есть, а ничего не работает, и что это еще за "err_msgs.res" :). Если же проблемы все же возникнут, не спеши писать мне или разработчикам. Попробуй сначала почитать install.txt.

После установки можно полюбоваться на палитру компонентов. Там прибавились целых три закладки (ZTV Tools, ZTV Compress, ZTV Decompress), содержащие суммарно 35 (тридцать пять) компонентов! Вот это, я понимаю, королевский набор для работы с архивами!

ZTV Compress

1) TBlackHole. Предназначен для создания blackhole (*.bh) архивов.
2) TGZip. Позволяет создавать gzip архивы. Очень полезная вещь для юниксоидов :).
3) TJar, TLha, TCab, TTar. Соответственно, создают Jar, Lha и Tar архивы.
4) TUUEEncode. Создает UUE/XXE кодированные файлы для емайла.
5) TZip. Собственно, самый главный компонент в нашем обзоре. Он создает PkZip совместимые ZIP архивы.

После того, как я рассказал, зачем, собственно, нужны компоненты этой вкладки, возникает резонный вопрос - как их использовать? Также неплохо бы рассказать о некоторых методах, свойствах и событиях.

Создается архив довольно просто. Надо присвоить свойствам ArchiveFile (тип string, это имя будущего или имеющегося архива) и FileSpes (тип TStrings, содержит список файлов, подлежащих архивации; также можно использовать маски типа *.*) вразумительные значения, а затем с помощью метода Compress запустить процесс запаковки. Он вернет тебе переменную типа integer. Это и будет количество заархивированных файлов. Также можно добавить еще и свойство Password. Это будет пароль для архива. Будь осторожен с прописными и строчными буквами - они различаются.

ZTV Decompress

1) TUnACE, TUnARJ, TUnBH, TUnCab. Распаковывают, соответственно, ACE, ARJ, BH (BlackHole) и MS Cab архивы.
2) TUnGZIP. Распаковывает .gz, .z, .tar .jz архивы.
3) TUnJar, TUnLha, TunRar, TunTar, TUnZip. Разархивируют Jar (Java Soft формат), Lha, Rar, Tar, ZIP.

Процесс распаковки мало чем отличается от паковки. Здесь необходимо присвоить соответствующие значения для ArchiveFile, FileSpec и ExtractDir (определяет директорию, в которую надо распаковывать) и запустить распаковку с помощью метода Extract. На этот раз он вернет тебе количество распакованных файлов. ВНИМАНИЕ! TUnACE и TUnRAR требуют для своей работы библиотеки: unace.dll и unrar.dll соответственно.

ZTV Tools

1) TArc2Arc. Конвертирует архивы из формата в формат. Для этого нам понадобятся некоторые данные.

Свойства:
ArchiveFile - здесь пишется имя старого архива.
NewArchive - имя нового архива.
OutArcType - тип нового архива; например: tyZip, tyBH, tyLzh, tyCab.
OutArcMethod - способ конвертации.
IntegrityCheck - проводить ли проверку нового архива (true/false).
DateAttribute - какую дату присваивать файлам из нового архива.
Может быть:
daFileDate - те же даты, что и у файлов исходного архива.
daSysDate - системную дату.
daMaxFileDate - дату самого нового файла из архива.
Это свойство годится также и всем остальным компонентам.
Методы:
Activate - запускает процесс.

2) TMakeSFX. Создает Sfx архив из обычного.

Свойства:
ArchiveFile - имя обычного архива.
TargetFile - имя будущего Sfx'a.
SfxStubDir - определяет директорию с *.sfx файлами. Они необходимы для работы компонента (например, чтобы из Zip'a сделать SFX, нужен ZTV_Zip.SFX), а путь к ним по умолчанию - c:\windows\system\.
Метод CreateSfx запускает весь этот процесс.

3) TZipTV. Как и любой телевизор, этот показывает интимные подробности из жизни архивов. То есть с его помощью можно выяснить практически любую информацию об архиве и содержащихся в нем файлах.

Свойства:
ArchiveFile - определяет имя архива-телезвезды :).
FileSpec.Add - маска для запакованных файлов. Тип данных - TStrings.
FilesInArchive - список заархивированных файлов, соответствующий маске из предыдущего свойства. Тип тоже TStrings.
Count - количество запакованных файлов.
TotalUnpackedSize - исходный размер файлов.
TotalPackedSize - размер запакованных файлов.
Метод:
GetFileInfo - получает информацию о заархивированном файле. Например, такую:
ArchiveFile - его имя.
Date - дата. Легко приводится в божеский вид при помощи функции FormatDateTime. Это делается, к примеру, так: FormatDateTime('mm-dd-yy', ZipTV1.Date). Она вернет тебе string, содержащий дату. То же самое и со временем.
PackedSize - его размер после паковки.
UnpackedSize - его исходный размер.
Ratio - compress ratio.
CRC - его CRC.

Вот такой веселый компонент. Если ты заглянешь в хелп-файл с именем tziptv.hlp, то узнаешь еще много нового.

4) TZipKey. Самый][-компонент в моем обзоре :). Дело в том, что он, так сказать, помогает вспомнить забытые пароли. Сам понимаешь, есть запароленный архив, а пароль забыл, ну или не знал... Но узнать-то хочется! Вот и вперед. Для этого компонента есть очень хорошее демо (\ZIPZV5\DEMO\ZIPKEY\) и его надо освоить. Строго говоря, для многих компонентов есть демо, но не все они так хороши. В нелегком хакерском деле нам содействуют:
ArchiveFile - имя жертвы.
FileSpec - все та же маска для файлов.
CharSets - способ поиска паролей. Например, если присвоить Zipkey1.CharSets:= TCharSets(0), то поиск ограничится паролями, состоящими только из цифр. Если же вместо нуля будет 8, то поиск будет идти по всем ASCII символам. Все значения ты сможешь узнать из демы (в ней все очень понятно сделано), поскольку в хелпе этого компонента почему-то нет. Между прочим, поиск можно вести и по словарю. Их можно скачать на сайте разработчика в разделе "о продукте". Есть даже китайский wordlist. Тебе он, безусловно, пригодится.

StartPassword - с него начинается поиск.
Методы:
Activate - запускает процесс.
Pause - делает паузу :).
Как только пароль находится, вызывается событие OnFound и свойство Password приобретает конкретное значение. Им и предстоит воспользоваться.
На этом с обзором я заканчиваю, так что перейдем к моему любимому кодингу.

Интерфейс

Создавай форму (БОЛЬШУЮ форму, пример будет немаленьким) и клади на нее 5 TEdit, 12 TLabel, 7 TButton, 2 TListBox, 2 TProgressBar, 1 TGroupBox. Поскольку так просто разобраться в этом многообразии не могу даже я, давай посмотрим на этот рисунок:

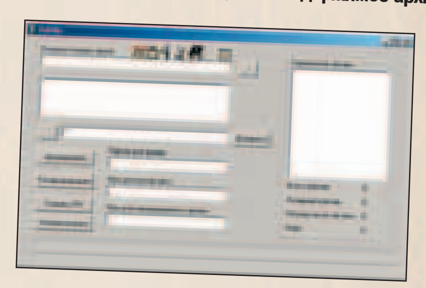


Так примерно и должен выглядеть наш новорожденный проект. Самое время раздать свойства. Вот такие:

label1 - caption "Открыть/создать архив:"
label2 - caption "Пароль для архива"
label3 - caption "Путь для распаковки"
label4 - caption "Путь для новорожденного архива"
label5 - caption "Всего файлов:"
label7 - caption "Исходный размер:"
label9 - caption "Размер после паковки:"
label11 - caption "Ratio:"

Label'ы же под номерами 6, 8, 12 должны получить вместо caption'а просто нули, поскольку нормальные значения они получат только в ран-тайме. Кстати, пока не поздно, предупреждаю. Оформлением формы можешь не заниматься, так как на диске лежат 2 исходника: оформленная, но неработающая форма (в образовательных целях) и полностью готовый проект для нетерпеливых. Ладно, продолжим дизайнерство, набивай дальше:

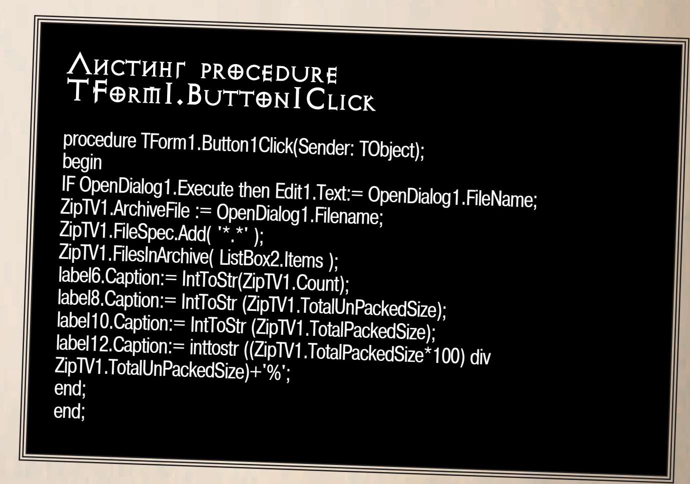
Button'ы под номером 1 и 2 получают caption в виде троеточия. А вот остальные:
Button3 - caption "Добавить!"
Button4 - caption "Архивировать"
Button5 - caption "Разархивировать"
Button6 - caption "Создать SFX"
Button7 - caption "Конвертировать"
GroupBox1 получает caption "Содержимое архива".



Также не забудь определить на форму компоненты: Zip, UnZip, Arc2Arc, MakeSfx и OpenDialog из закладки Dialogs.
Вот что у меня получилось в результате:

Кодинг forever

Вначале разберемся с открытием архива и экранизацией его интимных тайн :). Для этого взгляни онклик первой кнопки (с троеточием):



Листинг procedure TForm1.Button1Click

```
procedure TForm1.Button1Click(Sender: TObject);
begin
IF OpenDialog1.Execute then Edit1.Text:= OpenDialog1.FileName;
ZipTV1.ArchiveFile := OpenDialog1.Filename;
ZipTV1.FileSpec.Add( '*.*' );
ZipTV1.FilesInArchive( ListBox2.Items );
label6.Caption:= IntToStr(ZipTV1.Count);
label8.Caption:= IntToStr (ZipTV1.TotalUnPackedSize);
label10.Caption:= IntToStr (ZipTV1.TotalPackedSize);
label12.Caption:= inttostr ((ZipTV1.TotalPackedSize*100) div
ZipTV1.TotalUnPackedSize)+'%';
end;
end;
```

Как всегда все просто и занудно. Если пользователь выбрал имя файла, мы передаем его ZipTv, присваиваем маску *.* и выводим в ListBox2 файлы по этой маске. То есть все файлы из архива. Затем выводим дополнительную информацию об архиве: количество файлов, исходный размер данных, паковынный размер и, наконец, compress ratio. Дело в том, что разработчики компонента придумали для этой цели целую функцию CalcRatio. Но до ее использования я никогда не унижусь :). Принять исходный размер за 100% и вычислить, сколько же осталось, это под силу даже школьнику из приюта для олигофренов. И это будет одна и та же строчка кода, так что тяга к упрощению ущемлена не будет :).

NEXT

СВОЙ ZIP НА DELPHI

 Лозовский Александр (klouniz@mail.ru)

Архивариус

В первом listbox'е ты сможешь составить список файлов, подлежащих архивации. В этом нам поможет Edit2, Button2 и Button3 (которая "Добавить!", она добавляет содержимое Edit2 в ListBox1). Button2 же просто активирует OpenDialog и вводит имя файла в Edit2. Вот как это делается:

OnClick Button2:
ListBox1.Items.Add(Edit2.Text);
OnClick Button3:
ListBox1.Items.Add(Edit2.Text);

Впрочем, маски (типа *.exe, ??e.doc) тебе придется набивать в Edit2 уже вручную. Посмотрим на ОнКлик кнопки "Архивировать"

Листинг procedure TForm1.Button4Click

```
procedure TForm1.Button4Click(Sender: TObject);
var i: integer;
begin
Zip1.ArchiveFile:= Edit1.Text;
Zip1.FileSpec.Clear;
Zip1.FileSpec:= ListBox1.Items;
Zip1.Password:= Edit3.Text;
i:= Zip1.Compress;
ShowMessage (inttostr(i)+' файлов запаковано!');
end;
```

Переменная i будет содержать количество запакованных файлов. Далее мы определяем имя архива, соотносим содержимое ListBox1 со свойством FileSpec и вставляем пароль из Edit3. Запускаем процесс и выводим результат с помощью ShowMessage.

Разархивариус

Вот онклик кнопки "Разархивировать":

Листинг procedure TForm1.Button5Click

```
procedure TForm1.Button5Click(Sender: TObject);
Var i: integer;
begin
UnZIP1.ArchiveFile := Edit1.text;
UnZIP1.Filespec.Clear;
UnZIP1.FileSpec.Add('*.*');
UnZip1.Password:= Edit3.Text;
UnZip1.ExtractDir := Edit4.text;
i := UnZIP1.Extract;
ShowMessage (inttostr(i)+' файлов распаковано!');
end;
```

Здесь все очень похоже на паковку, кроме нового свойства ExtractDir, данные для которого берутся из Edit4.

Создаем

Создать SFX архив из обычного не просто, а очень просто. Делается это в 3 строчки кода. Я имею в виду вот эти строчки:

MakeSfx1.ArchiveFile:= Edit1.Text;
MakeSfx1.TargetFile:= Edit5.Text;
IF MakeSfx1.CreateSfx then ShowMessage ('Архив создан!');

Это и есть Онклик от кнопочки "Создать SFX". Путь к конечному файлу будет определяться содержимым Edit5. Не забудь, что по умолчанию SFX файлы ищутся в системном каталоге.

Конвертируем

Вот как это делается:

Листинг procedure TForm1.Button7Click

```
procedure TForm1.Button7Click(Sender: TObject);
begin
Arc2Arc1.ArchiveFile := Edit1.text;
Arc2Arc1.NewArchive := Edit5.Text;
Arc2Arc1.OutArcType := tyZip;
Arc2Arc1.OutArcMethod := amCreateNew;
Arc2Arc1.IntegrityCheck := True;
Arc2Arc1.DateAttribute := daFileDate;
Arc2Arc1.Activate;
end;
```

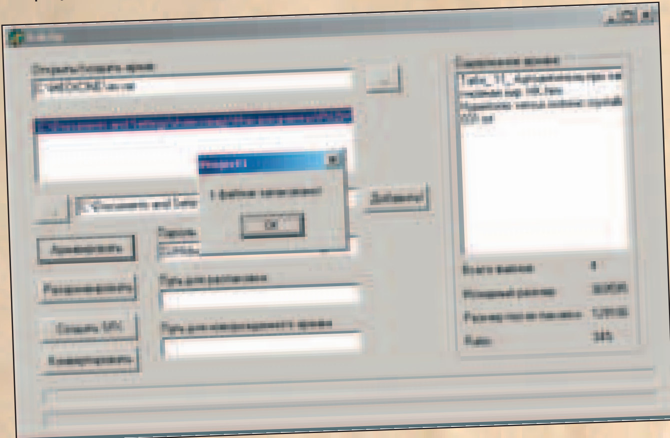
Если ты внимательно читал теорию, то уже все понял: здесь я последовательно определяю исходный и конечный файлы, выбираю способ конвертации. Вот, собственно, и весь пример. Самое время чуть-чуть его модернизировать. Не зря же я положил на форму 2 TProgressBar :).
Создай для компонента TZip1 событие OnProgress и вбей туда следующее:

ProgressBar1.Position := ProgressByFile;
ProgressBar1.Update;
ProgressBar2.Position := ProgressByArchive;
ProgressBar2.Update;

Эти простые строчки обеспечат пользователю наблюдение за двумя важными процессами: прогрессом в архивации текущего файла и архива в целом.

Клинические испытания

Я запустил нашу прогу и открыл один из своих архивов, получив краткую информацию о нем. Затем у меня появилось желание добавить в него файлик, что я и сделал с неплохим результатом - compress ratio был что-то около 34%.



Готово к употреблению!

В данной ситуации это нормально для ZIP алгоритма в любой его реализации. А вот RAR справился лучше - 25% и никаких гвоздей. До сих пор удивляюсь популярности WinZip. Неужели Drag'n'Drop так притягивает пользователей?

Final Prayer

Вот и все на сегодня. Остальное оставляю на откуп читателям: чтение хелп-файла к компонентам (правда, там есть не все и он на английском) и освоение демо. После этого можно будет считать себя компетентным специалистом в области архивирования данных. Без дураков - ведь заказчику неважно, КАК ты будешь делать прогу. Важно, КАК СКОРО она будет написана и НАСКОЛЬКО ФУНКЦИОНАЛЬНА она будет. Как говаривал Horrific : "Не надо изобретать велосипед и терять время, переписывая то, что сделано до тебя в виде компонентов".
Да, у меня есть еще одна хорошая новость. Теперь ты сам можешь предложить тему для "Кодинга". И вполне возможно, что именно ее ты и увидишь в очередном][. Все свои идеи сливай мне на klouniz@mail.ru.



TM RADIO ULTRA

Носки!

Миниатюрный сокс-сервер

Прокси. Это слово знакомо каждому интернетчику. Его знает любитель поругаться грязными словами в чатах, им пользуются мерзкие кардеры в поисках бесплатного стафа, и уж тем более проксю юзают всеми любимые скрипткидисы, им ведь тоже необходимо иметь анонимность в Сети. А иначе, какие же они "хакеры"? :)

Николай "GorluM" Андреев (gorlum@real.xakep.ru)

На самом деле полезность прокси бывает разной. Например, у тебя в доме настроена локалка, а на одном из компьютеров есть выход в интернет. Чтобы все остальные компы тоже смогли выползать в инет, тебе придется выполнить одно из следующих действий: поставить NAT, что может сделать далеко не каждый, установить обычный роутер, но для этого понадобится выделить подсеть IP-адресов, и самый распространенный выход - установить проксю. Причем последний вариант - самый простой в реализации. Но ты можешь возразить, сказав, что не весь сетевой софт будет работать с проксей. Доля правды в этом есть, но фактически прокси поддерживает весь популярный софт: mIRC, ICQ, Opera, Internet Explorer. Вряд ли ты сможешь найти известное сетевое приложение без возможности использования прокси. Так что ты будешь устанавливать именно проксю, причем не какой-нибудь WinGate, а собственную реализацию. Да-да, собственную! Этот урок программирования на C/C++ посвящен написанию своего прокси-сервера.

В качестве протокола нашего сервера мы будем использовать socks4. Несложный в реализации и широко распространенный, он оптимален для нашей задачи. А задача наша - написать прозрачный (не анонимный) прокси-сервер, работающий с большинством сетевых приложений. Причем, весить он будет всего 2.5 Кб, что позволит использовать его в любых проектах.

Немного RFC

Идея программы проста до безобразия. Создаем порт-сервер и ждем подключений. При соединении принимаем некоторую информацию от клиента, содержащую версию протокола, ip и порт, на которые необходимо законнектиться. Инфу о пользователе и просьбы пройти аутентификацию мы просто пропускаем. Оно нам не нужно. Если вдруг понадобится, ты сам сможешь это реализовать, почитав RFC1928.
Итак, необходимую информацию мы записываем в структуру tag_SOCKS4_REQUEST:

```
typedef struct tag_SOCKS4_REQUEST{
        unsigned char ucVersion;
        unsigned char ucCommand;
        WORD wDestPort;
        DWORD    dwDestIp;
} SOCKS4_REQUEST;
```

Заметь, IP принимается как DWORD (двойное слово, 4 байта). Чтобы использовать его в функции connect, нам придется преобразовать это значение в тип IN_ADDR. IN_ADDR - это те же 4 байта, только разделенные в структуре. Удобнее всего сделать преобразование с помощью функции memcpy (A,B,C), которая выполняет копирование куска памяти длиной C из A в B, где A - указатель "куда" копировать, а B - "откуда".

Игнорировать ненужную нам информацию, мы будем с помощью дополнительной функции. Она будет читать из порта по байтику до тех пор, пока не придет завершающий символ - '\0'. Вот эта функция:

```
void FlushRecvBufferUntil(SOCKET s, char condition){
        int iReceiveRes; char cDummy;
        do iReceiveRes = recv(s, &cDummy, sizeof(cDummy), 0);
        while (iReceiveRes != SOCKET_ERROR && iReceiveRes != 0 &&
cDummy != condition);
}
```

Нулевой байт будет означать, что клиентский sock4-запрос окончен, и нашему проксику пора соединиться с адресом назначения dwDesIp. Если соединение прошло успешно, мы создаем канал данных между начальным и конечным пунктом. Если же соединение не удалось, то сервер просто убьет созданный ранее сокет при помощи WinSock-функции closesocket.

Пишем

Для работы sock4-сервера, помимо главного потока, создающегося из EntryPoint винды (в нем мы слушаем порт), нам потребуется еще один поток. Через него будет производиться коннект и пересылка данных от отправителя к получателю.

Из статьи в][12.02 "Пишем своего трояна" ты уже должен знать, как создавать сокет и слушать порт. На этот раз нам придется немного модифицировать механизм приема новых соединений. Функцию accept, ожидающую подключений на указанный порт и возвращающую сокет, мы должны будем запихнуть в бесконечный цикл. А в самом цикле при новом соединении создадим тред и передадим ему полученный сокет. Выглядит это так:

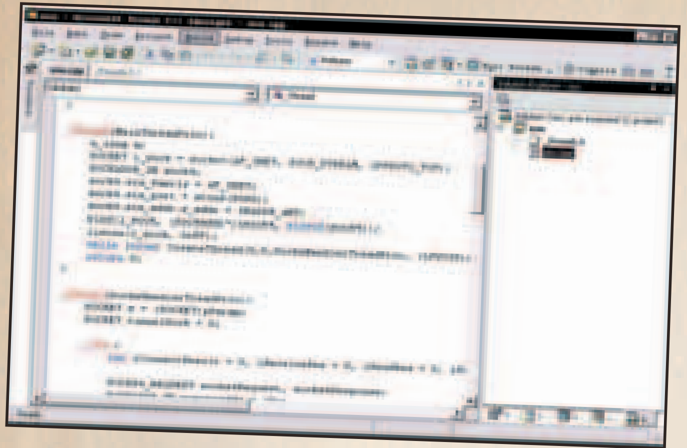
```
while (true) {
 CreateThread(0,0,secthread,(LPVOID)accept(s, 0, 0), 0, &a);
}
```

где secthread - имя треда для обработки соединения, s - сокет, слушающий порт. Теперь, если кто-то приконнектится к открытому порту, сервер создаст нить (thread), в которую передаст переменную типа SOCKET для работы с новым соединением.
С главным потоком все ясно, а вот как обстоят дела с побочным, мы сейчас выясним. Для более удобного объявления треда я создал небольшой макрос:

```
#define _Thread(x) unsigned long __stdcall x (LPVOID pParam)
```

И теперь, если необходимо создать тред, достаточно написать: _Thread (имя_нити). Но на этом способе облегчения кодинга я не остановился. Пользуясь Visual Studio .NET, я от-

копал немало очень интересных для си-кодера фишек. Вот одна из них: user keyword, по-русски - пользовательские ключевые слова. Они позволяют выделить в VS определенные слова каким-нибудь цветом (см. скрин).



user keywords выделяются красненьким

Я ими активно пользуюсь и тебе советую. Если ты юзаешь свои макросы, то очень удобно сделать их выделяющимися в тексте программы. Для добавления ключевых слов достаточно создать файл usertype.dat в директории, где лежит твоя VS.NET, в Common7\IDE, и записать notepad'ом в него нужные ключевые слова по одному в строке. После этого перезагрузи VS.NET и радуйся красивому сорцу.

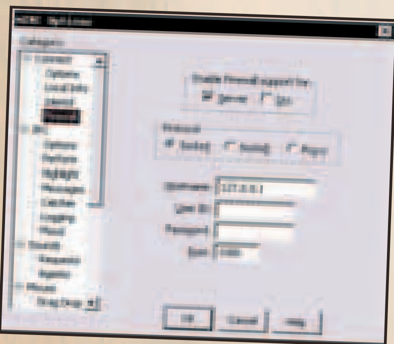
Но вернемся к нашим баранам. В созданной нити мы будем обрабатывать входящие соединения и при необходимости создавать новые коннекты с серверами, указанными в запросах. Вот как это происходит. Сначала принимаем один байт, в нем содержится версия требуемого сокс-протокола. Причем получим этот байт, не удаляя его из очереди сообщений. Для этого при вызове winsock-функции recv в четвертом параметре передадим значение MSG_PEEK. Теперь, при следующем чтении из сокета, мы сначала получим этот же байт и только потом все остальное. Это необходимо для отброса лишних байт при проверке версии. Итак, если версия равна четырем, то заполним структуру socks4Request типа SOCKS4_REQUEST из нашего сокета:

```
recv(s, (char*)&socks4Request, sizeof(socks4Request), 0);
```

Далее запустим функцию FlushRecvBufferUntil, с помощью которой пропускаем мимо ушей все лишнее, что хочет сообщить нам клиент. И только когда заголовок запроса к прокси полностью принят (пришел '\0'), мы попытаемся сконнектиться с dwDestIp (его получили из запроса).

При успешном соединении создаем бесконечный цикл, в котором будем совершать обмен данными в обоих сокетах: полученных accept`ом и connect`ом. С помощью функции select и пары макросов проверим, есть ли данные в сокетах. Для этого сначала создадим переменную типа fd_set, потом макросом FD_ZERO обнулим ее, а FD_SET'ом добавим к ней указатель на сокет, из которого будем читать данные. Теперь, вызвав функцию select и передав во втором параметре нашу переменную, мы можем воспользоваться макросом FD_ISSET. С его помощью мы узнаем состояние очереди чтения. И только когда она не пуста, читаем данные из одного сокета и пишем их в другой.

Поскольку мы хотим выполнять эти действия в одном цикле и в одном потоке, нам надо избавиться от одного нежелательного эффекта. Дело в том, что функция recv останавливает нить, из которой запущена, и ждет получения данных. Если в момент такой остановки придут данные в другой сокет, наша программа не сможет их перенаправить, так как будет занята. Как выяснилось, выйти из этого положения довольно просто. Нашим сокетам необходимо сообщить некоторый параметр, заставляющий recv и другие подобные функции выполняться в отдельном потоке. Вот как это выглядит в нашей программе:



Настраиваем мирк на работу с нашей проксей

```
u_long ulVal = 0;
ioctlsocket(s, FIONBIO,
&ulVal);
```

Сокеты, не останавливающие нить до конца выполнения той или иной операции, называются неблокирующими.

Если соединение рвется или происходит какая-либо ошибка, то цикл завершается, оба сокета закрываются, а нить заканчивает свое существование.

Break

Вот и все. Как видишь, такая полезная программа очень проста в написании. Осталось только вставить пару строк для уменьшения размера exe'шника. Получившийся прокси прекрасно работает со всеми приложениями, которые я смог найти у себя на винте. ICQ сначала ругалась, но потом я отрубил работу DNS через firewall, и все заработало.

Сам проект для Visual Studio .NET и полный исходный текст программы, а также скомпилированный exe'шник ты можешь взять на диске или скачать с сайта www.xakep.ru. Если возникли какие-то вопросы, идеи или замечания - пиши. Постараюсь ответить.

Удачного компилирования.

Листинг потока для обработки соединений

```
_Thread(SocksHandlerTreadProc){
SOCKET s = (SOCKET)pParam;
SOCKET tunnelSock = 0;
_try {
 int iConnectResult = 0, iReceiveRes = 0, iSendRes = 0, iSocketsSet = 0;
 SOCKS4_REQUEST socks4Request, socks4Response;
 SOCKADDR_IN remoteAddr = {0};
 fd_set fds_read;
 FD_ZERO(&fds_read);
 FD_SET(s, &fds_read);
 TIMEVAL tv = {0};
 tv.tv_sec = 30;
 char cSocksVersion = 0;
 int iSelectResult = select(0, &fds_read, NULL, NULL, &tv);
 if (iSelectResult == SOCKET_ERROR || !iSelectResult) _leave;
 u_long ulVal = 0;
 ioctlsocket(s, FIONBIO , &ulVal);
 iReceiveRes = recv(s, &cSocksVersion, 1, MSG_PEEK);
 if (cSocksVersion == 4){
  iReceiveRes = recv(s, ((char*)&socks4Request), sizeof(socks4Request), 0);
  if (iReceiveRes == SOCKET_ERROR) _leave;
  ulVal = 1;
  ioctlsocket(s, FIONBIO , &ulVal);
  FlushRecvBufferUntil(s, '\0');
  if (socks4Request.ucCommand == 1){
   ulVal = 0;
   ioctlsocket(s, FIONBIO, &ulVal);
   remoteAddr.sin_family = AF_INET;
   memcpy(&(remoteAddr.sin_addr),&(socks4Request.dwDestIp),
sizeof(remoteAddr.sin_addr));
   remoteAddr.sin_port = socks4Request.wDestPort;
   tunnelSock = socket(AF_INET, SOCK_STREAM, 0);
   iConnectResult = connect(tunnelSock, (struct sockaddr*) &remoteAddr,
sizeof(remoteAddr));
   if (iConnectResult != SOCKET_ERROR){
    socks4Response.ucCommand = 90;
    socks4Response.ucVersion = 0;
    iSendRes = send(s, (char*)&socks4Response, sizeof(socks4Response), 0);
   } else _leave;
  } else _leave;
 } else _leave;
 ulVal = 0;
 ioctlsocket(tunnelSock, FIONBIO, &ulVal);
 ioctlsocket(s, FIONBIO, &ulVal);
 char swapBuffer[4096*16];
 int iSendResult, iRecvResult;
 tv.tv_sec = 2;
 while (true){
  FD_ZERO(&fds_read);
  FD_SET(s, &fds_read);
  FD_SET(tunnelSock, &fds_read);
  iSocketsSet = select(0, &fds_read, NULL, NULL, &tv);
  if (iSocketsSet > 0){
   if (FD_ISSET(s, &fds_read)){
    iRecvResult = recv(s, swapBuffer, sizeof(swapBuffer), MSG_PEEK);
    if (iRecvResult == 0) _leave;
    else iRecvResult = recv(s, swapBuffer, sizeof(swapBuffer), 0);
    if (iRecvResult != SOCKET_ERROR && iRecvResult > 0 )
     iSendResult = send(tunnelSock, swapBuffer, iRecvResult, 0);
    else _leave;
   }
   if (FD_ISSET(tunnelSock, &fds_read)){
    iRecvResult = recv(tunnelSock, swapBuffer, sizeof(swapBuffer), MSG_PEEK);
    if (iRecvResult == 0) _leave;
    else iRecvResult = recv(tunnelSock, swapBuffer, sizeof(swapBuffer), 0);
    if (iRecvResult != SOCKET_ERROR && iRecvResult > 0 )
     iSendResult = send(s, swapBuffer, iRecvResult, 0);
    else _leave;
   }
  }
 }
}
}
if (s) closesocket(s);
if (tunnelSock)closesocket(tunnelSock);
return 0;
}
```

Никита "red_ion" Кислицин (nikitoz@real.xakep.ru)
http://nikitos.inc.ru

Показывай грамотно!

В предыдущем номере мы открыли тему создания баннеропоказной системы. Существенное внимание было уделено производительности создаваемых сценариев. Сегодня же мы допишем эту систему, а чтобы разнообразить материал, мы поговорим еще о защите от накруток, об организации хитрого таргетирования показов и вообще о специфике создания таких вот систем. Также с этого номера я решил в каждом выпуске обязательно освещать основные новости веб-программирования: появление новых версий вебсерверов, интерпретаторов, патчей к найденным дыркам и т.д. Welcome aboard…

Никита "red_ion" Кислицин (nikitoz@real.xakep.ru) http://nikitos.inc.ru

Что там внутри?

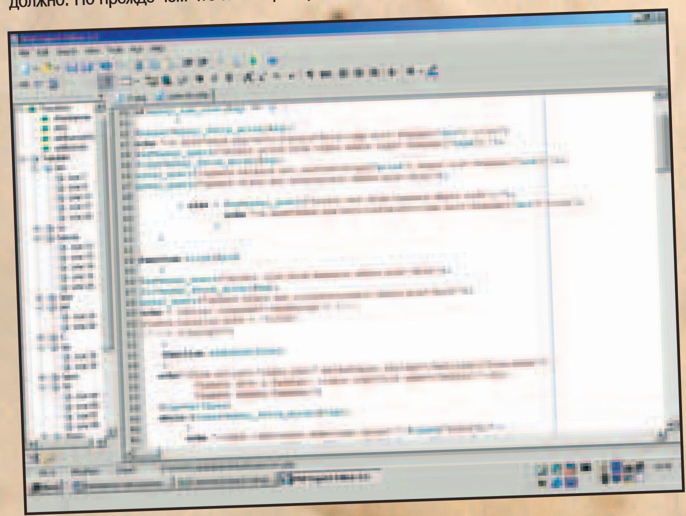
Как я уже говорил, система будет представлять собой шесть скриптов, три из которых модульные - в них описываются все используемые функции, а оставшиеся юзают эти процедуры и осуществляют взаимодействие с пользователем. Некоторые функции по работе с клиентом мы уже описывали при создании site-engine, а в прошлом выпуске рассмотрели показ заданного баннера и обработку клика по нему. Напомню, наша система рассчитана на работу с большим количеством рекламодателей, каждый из которых может иметь по несколько баннеров одного и того же формата. Как же определить, какой баннер показывать? Вообще, в нормальных системах выбор делается исходя из таргетинговых соображений: рекламу мониторов показывают людям, у которых низкое разрешение экрана, дорогие машины предлагают пользователям с хорошим дисплеем и проживающим в крупных городах, и т.д. и т.п. Но у нас безтаргетинговая система, поэтому в качестве определяющей величины будет выступать количество купленных для каждого баннера показов. Оно и логично: чем больше денег потратил перец, тем выше у него приоритет :). Еще раз опишем таблицу с баннерами:

```
mysql> create table banners(
-> bid int not null auto_increment primary key, #идентификатор баннера
-> type int, # идентификатор типа этого баннера
-> uid int, # идентификатор владельца баннера
-> link varchar 100, # линк, куда ведет баннер
-> src varchar 100, # путь, по которому находится картинка баннера
-> shows int); # количество показов
```

Функцию, определяющую, какой из баннеров надо показывать, зададим следующим образом: function show(tid : int):int. Вот как она работает. Составляется sql-запрос вида "select bid from banners order by shows limit 1". Он вернет указатель на один баннер, имеющий наибольшее число показов. Возвращаемый идентификатор баннера выводится при помощи уже описанной нами функции showbanner(pid). Понятно, что такой алгоритм выборки не является оптимальным. Ведь если кто-то купил кучу показов, то будет высвечиваться один и тот же баннер, а мелкие заказчики будут сосать лапу. Это не есть гуд. Поэтому в более сложных и продуманных системах используются хитрые вытесняющие приоритетные алгоритмы выборки. Например, добавляется еще одно поле "priorithet", содержимое которого в начальный момент зависит от числа купленных показов. После показа баннера с самым высоким приоритетом, эта величина снижается, у остальных наоборот повышается. Таким образом, через некоторое время, даже если у баннера будет еще очень много показов, его приоритет понизится, и в итоге высветится другой баннер. Так сказать, он "всплывет", а потом "утонет". И так будет повторяться. Но мне сейчас меньше всего хотелось бы останавливаться на этих алгоритмах. Ты их и сам сможешь без труда составить, посидев с листочком бумаги и карандашом :).

Интерфейс

Сейчас же следует обговорить интерфейс рекламодателя и описать функции по взаимодействию с ним. Процедуру аутентификации мы позаимствуем из статьи "Система контент-менеджмента". В результате чего останется описать следующие функции: addbanner(tid, oid, shows, src, link); editbanner(bid, shows, src, link); delbanner(bid); edituser(login, password, name, organisation, telephone, email, address). Функция addbanner будет использовать библиотеку Бутелла, предоставляющую целый набор API для работы с графическими файлами. Поддерживается как создание новых, так и модификация уже существующих изображений. Нам же понадобится лишь одна функция GetImageSize(filename), возвращающая размеры изображения. Эта библиотека обычно уже входит в поставку php, так что проблем с ее использованием возникнуть не должно. Но прежде чем что-либо проверять, надо это "что-то" загрузить на сервер.



Кодим скрипт

Загружать изображения клиент будет через обычную форму (напомню, что среди объектов, которые могут быть отправлены post-запросом, есть и файл - это поле вставляется в хтмл-документ тегом <input type=file name=filename>). Первым делом нам следует проверить соответствие картинки параметрам, определенным в таблице types для баннеров этого типа. Ведь если пользователь вставит мастодонта размером 468*60 в узенькую таблицу, рассчитанную на кнопку размером 81*33, ничем хорошим это не закончится. В случае, когда загружаемое изображение соответствует стандарту, мы добавляем в таблицу с баннерами соответствующую запись, после чего реклама начинает отображаться посетителям сайта.

Функция editbanner выполняет аналогичные проверки, после чего модифицирует запись в таблице. Остальные же процедуры довольно банальны и особого интереса не представляют.

Функции администрирования системы, т.е. управление рекламодателями, абсолютно идентичны уже описанным процедурам работы с базами данных, которых мы наделали больше чем достаточно. Так что ты и сам можешь их описать: добавление, модификация и удаление пользователя, аналогичные функции по работе с баннерами пользователя. Особое внимание следует уделить безопасности, потому как в этом проекте ты уже имеешь дело с деньгами, а это серьезно :). Надо проверять все действия клиента, тщательно выписать процедуру проверки наличия денег на его счету и вообще все процедуры, работающие с базой данных. Ведь при помощи изощренного sql-injecting'а злоумышленник может натворить совсем мерзкие гадости :/. Код системы ты найдешь на cd и моем сайте, там же находятся все предыдущие статьи. Это на случай, если ты что-то не читал.

Функция добавления баннера

```
function addbannerform()
          {
  echo"<form action=\"index.php\" method=post enctype=\"multipart/form-data\">
   Укажите путь к баннеру: <input type=file name=\"banner\"><br>
  Укажите размер баннера:";
  $typ=GetTypes; # Получаем все существующие типы баннеров
  while($types=mysql_fetch_array($typ)) // Поскольку типов много, организуем
цикл по всем возвращенным записям БД
          {
     echo "<input type=radio name=type value='".$types["width"]."'>
     <input type=option ".$types["width"]."x".$types["height"]."<br>\n";
   }
  echo "Введите количество показов: <input type=text name=hshows
value=0><br>\n";
  echo "<input type=submit><br> </form>\n";
  }

function addbanner($tid, $shows, $src, $link)
          {
$wid=GetWidth($tid); # Получаем ширину изображения
$hei=GetHeight($tid); # Получаем высоту изображения
$uid=GetUidByLoginInfo($login, $passwd); # Получаем uid пользователя по его
логину и паролю
$size=GetImgSize($src); #
if(($wid==$size[0]) && ($hei==$size[1])) # Проверяем соответствие баннера
стандарту
                    {
     $sql="insert into banners values (null, '$tid', '$uid', '$link', '$src', '$shows')";
     if (mysql_query($sql)) {echo "Баннер добавлен в систему ротации!";}
     } else {echo "Баннер не соответствует указанному типу!";}
 }
```

Что такое таргетинг, и как его реализовать?

Таргетинг. Дословно переводится как "прицеливание". Под этим термином, применительно к рекламным технологиям, понимается разделение рекламной аудитории на группы по некоторому признаку: территориальному, финансовому, возрастному, половому, социальному и т.д. После того как аудитория поделена на группы, определяется потребитель продвигаемого товара или услуги. И реклама осуществляется лишь среди этой группы людей. Порой это в десятки, а то и в сотни раз эффективней, чем тупая реклама без таргетинга. И естественно, таргетирование крайне выгодно рекламным площадкам - стоимость таких показов гораздо выше обычных. Так что "targeting" - это эффективное разделение всей аудитории сайта на группы с целью повышения отклика от рекламы и съема дополнительных денежных знаков с рекламодателя :).

Осуществляется эта функция примерно следующим образом. При помощи JavaScript получаем массу полезной информации о клиенте: разрешение экрана, глубина цвета, ОС, браузер и т.д. По ip-адресу определяем примерное местоположение клиента (хорошо, если он не пользуется угрвайскими прокси-серверами). Далее чекается текущее время, день недели, а также адрес сайта, с которого человек пришел. Исходя из всей собранной информации составляется запрос на выборку наиболее подходящего баннера (критерии выборки своей рекламы определяет сам рекламодатель). Проще всего показы таргетировать поисковикам: на запрос "выделенные линии в Москве" показывать рекламу Зенона, а на "глазированные сырки оптом" реагировать баннером от Ростагроэкспорта :).

Как защититься от накрутчиков?

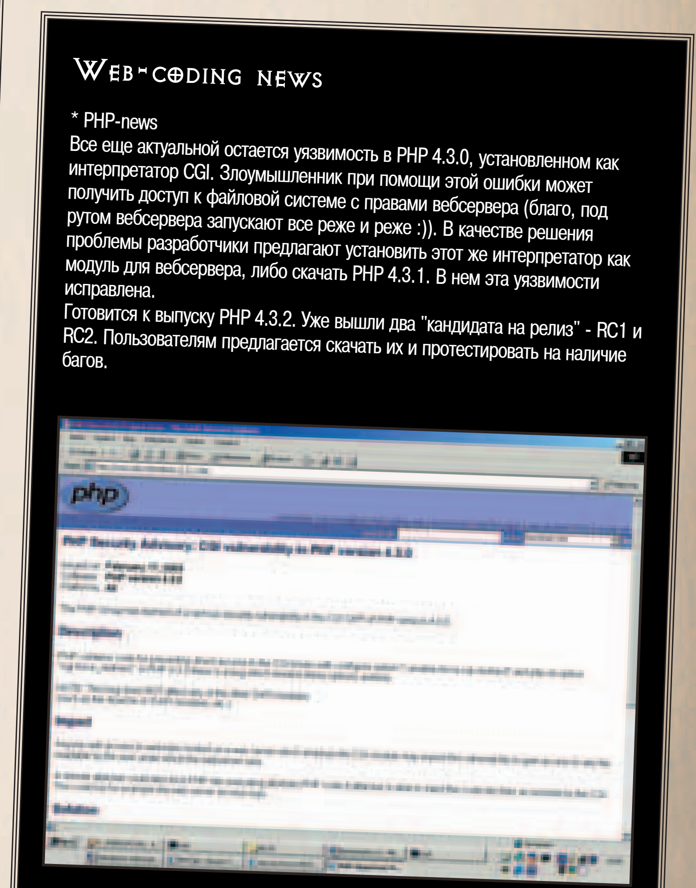
Если тебе доведется писать баннерообменную сеть, т.е. систему, в которой рекламодатель одновременно является и рекламной площадкой, то ты непременно столкнешься с проблемой накрутчиков. Это такие недобросовестные люди, имитирующие большой рекламный трафик при помощи специальных программ. Как этому противостоять? Наиболее простое и эффективное решение - просто не начислять показ, если от одного ip приходит более пяти (10,15,20...) запросов в минуту. Также следует игнорировать показы пользователям, не принимающим кукисы. Вообще, в таких делах следует отдавать приоритет именно системе, а не клиенту. Даже если ты не засчитаешь ему 1-3% от реальных показов, то ничего страшного не произойдет. Можно сказать, что это "комиссионные сборы" :). А вообще, сейчас накрутчиков становится все меньше и меньше, т.к. занятие это неблагодарное, да и сами системы стали более навороченными. Так что залогом хорошей посещаемости является именно качественная содержательная часть сайта, а не позиция в рейтинге. Хотя и без позиции тоже никуда :).

Web-coding news

* PHP-news

Все еще актуальной остается уязвимость в PHP 4.3.0, установленном как интерпретатор CGI. Злоумышленник при помощи этой ошибки может получить доступ к файловой системе с правами вебсервера (благо, под рутом вебсервера запускают все реже и реже :)). В качестве решения проблемы разработчики предлагают установить этот же интерпретатор как модуль для вебсервера, либо скачать PHP 4.3.1. В нем эта уязвимости исправлена.

Готовится к выпуску PHP 4.3.2. Уже вышли два "кандидата на релиз" - RC1 и RC2. Пользователям предлагается скачать их и протестировать на наличие багов.



Уязвимость в PHP 4.3.0

* Apache news

Вышел Apache 2.0.42 - один из вариантов 2-ой версии. Основные отличия от 1.3 - переработанные модули, улучшенная поддержка многопоточных Unix-систем, а также более стабильная работа на Windows и OS/2-платформах. Разработчики уделили внимание упрощению процесса установки и конфигурации самого вебсервера, добавили поддержку ipv6 и многоязычных технологий (так, например, сообщения об ошибках теперь могут выводиться на разных языках).



ЗАЛ СУДА

Stepan Ilyin aka Step (step@real.xakep.ru)



Урожденная	Postal 2
Жанр	FPS
Похожесть	Blood 2
Мать/отец	Running With Scissors/Whiptail Interactive
Требует	P3-750(P4-1700), 128(512), 3D
Групповуха	Обломись

Описуха Безбашенный шутер с большим количеством извращений и насилия. Сюжет прост до безобразия: проживи 4 дня, решая обычные бытовые проблемы. Казалось бы, что может быть проще? Однако главный герой попадает в такое количество передряг и переделок, что мало не покажется. Так что бери в руки лопату, биту или молоток, чтобы раз и навсегда расправиться с нарушителями твоего внутреннего спокойствия.





ПРИГОВОР ХОРОШО

Урожденная	Grand Theft Auto: Vice City
Жанр	Гонки
Похожесть	GTA 3
Мать/отец	Rockstar Games/Rockstar North
Требует	P3-750(P4-1700), 128(512), 3D
Групповуха	Нужен специальный плагин

Описуха Разработчики "GTA: Vice city" предлагают нам окунуться в Америку 80-х годов, а точнее в огромный город Майями, полный мафиозных разборок, убийств и бесчинств, в которых ты играешь далеко не последнюю роль. Переработанный графический движок, абсолютно новый город, отличные саундтреки, новые виды передвижения (мотоциклы - rulezZz 4ever) и разнообразнейшие миссии наверняка доставят тебе немало удовольствия.

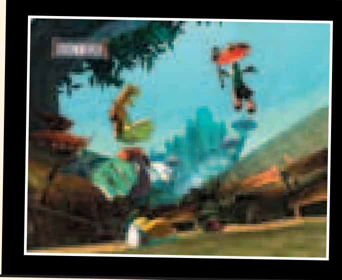


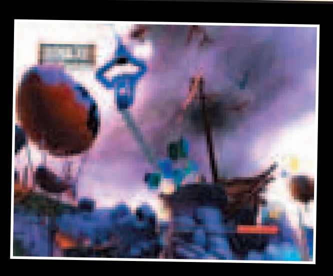


ПРИГОВОР РУЛЕЗ

Урожденная	Rayman 3: Hoodlum Havoc
Жанр	3D-аркада
Похожесть	Rayman 2
Мать/отец	Ubi Soft/Ubi Soft
Требует	P3-600(P3-1000), 128(256), 3D
Групповуха	Обломись

Описуха Общая тенденция такова: жанр 3D-аркады потихоньку умирает. Именитые разработчики почему-то обходят его стороной, а пародии на игры, выпускаемые полупрофессионалами, заранее обречены на провал. И вот чудо! Вышел RayMan 3. Ubi Soft'у удалось выпустить изумительную аркаду, прекрасно реализовать мультяшный мир, в точности передав его атмосферу, и написать логический и увлекательный сторилайн.



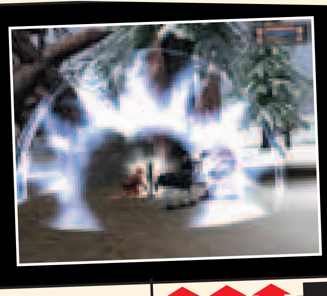


ПРИГОВОР ХОРОШО

Урожденная	Shadowbane
Жанр	3D on-line RPG
Похожесть	Ultima Online, AC2
Мать/отец	Wolfpack Studios/Ubi Soft
Требует	P3-700(P4-1500), 128(512), 3D
Групповуха	Инет

Описуха Главным плюсом игры является сбалансированность online-геймплея. Первоначально персонаж находится в безопасной зоне: здесь его не могут тронуть другие игроки. Но по достижении определенного уровня срок "бесплатной страховки" заканчивается, и перед игроком открывается просторы боев с другими персонажами. Невероятно продуманная, интересная и красивая игра. А самое главное - на модеме не тормозит!



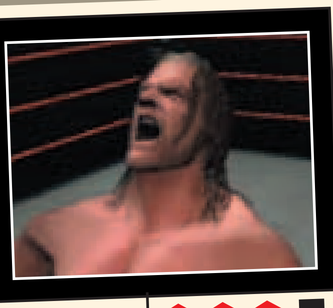


ПРИГОВОР ХОРОШО

Урожденная	WWE RAW
Жанр	Реслинг
Похожесть	WWF Wrestlemania
Мать/отец	Anchor, Inc., Jakks Pacific/THQ
Требует	P3-500(P3-800), 128(256), 3D
Групповуха	LAN

Описуха Смотрел трансляции реслинга по телевизору, сопровождаемые веселыми комментариями Николая Фоменко? Так вот эта игра представляет собой то же самое, только на компьютере. В игре представлено огромное количество спортсменов (а как их еще назвать?), каждый из которых обладает базовыми и коронными приемами. Плюс к этому: отличная графика, хорошее звуковое сопровождение и НЕВЕРОЯТНЫЙ геймплей.





ПРИГОВОР ХОРОШО

№ 0014

Урожденная	Port Royale
Жанр	*Экономический сим*
Похожесть	*Patrician 2*
Мать/отец	*Ascaron/Ascaron*
Требует	*P2-450(P3-600), 64(128), 3D*
Групповуха	*LAN, инет*
Описуха	Со всех сторон очень неплохой экономический симулятор, сохранивший все плюсы своего предшественника и одновременно порадовавший оригинальными нововведениями. Используя особенности сюжетной линии, ты можешь стать как законопослушным торговцем на море, так и беспощадным пиратом, или вообще начать военную карьеру. Так что скучать не придется, особенно учитывая отличную графику и звук.
ПРИГОВОР	ХОРОШО

Урожденная	TOCA Race Driver
Жанр	*Гонки*
Похожесть	*V8 Challenge*
Мать/отец	*Codemasters/Codemasters*
Требует	*P3-600(P3-1000), 128(256), 3D*
Групповуха	*В ассортименте*
Описуха	Средненькие гоночки. Да, автомобили воспроизведены бесподобно (причем как внешний вид, так и физика). Да, разработчики предлагают нам полтора десятка самых разнообразных и довольно красивых трасс. Да, звуком воющих моторов и саундтреками занимались люди, отлично знающие свое дело. Но нет в игре изюминки, особенностей. Все сделано добротно, но уж слишком стандартно. Нет драйва, нет и интереса...
ПРИГОВОР	СРЕДНЕ

ЗАЛ СУДА

Stepan Ilyin aka Step (step@real.xakep.ru)



Урожденная	Delta Force: Black Hawk Down
Жанр	FPS
Похожесть	Серия Delta Force
Мать/отец	NovaLogic/ NovaLogic
Требует	P3-600(P4-1,3GHz), 128(256), 3D
Групповуха	LAN, инет
Описуха	Очередной представитель уже поднадоевшей серии DF. По-моему, единственным положительным моментом является стремление разработчиков максимально правдоподобно передать исторические события в Сомали 1993 года. В остальном же - полный провал. Графических улучшений нет и в помине. Звуком, похоже, занимались дилетанты. А абсолютное большинство игровых моментов напоминают скорее аркаду, нежели тактический FPS.
ПРИГОВОР	ПЛОХО



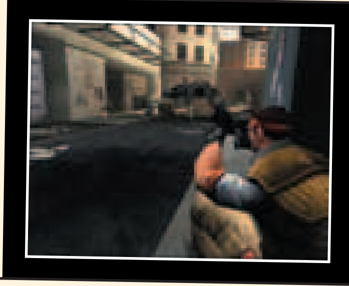


Урожденная	Jurassic Park: Operation Genesis
Жанр	Экономический сим
Похожесть	ZT: Dinosaur Digs
Мать/отец	Blue Tongue Software/Universal Interactive
Требует	P3-500(P3-1000), 128(256), 3D
Групповуха	Обломись
Описуха	Создание однообразных зоопарков, аквапарков и тому подобных мест отдыха, напичканных по самое не хочу различными аттракционами, закусочными и бутиками с сувенирами, уже порядком надоело. Именно поэтому "JP: Operation Genesis" привлек мое внимание. Разработчики предлагают нам нанять ученых, изучить ДНК динозавров и отстроить уникальный динопарк. Отличная идея и блестящая реализация.
ПРИГОВОР	ХОРОШО





Урожденная	Red Faction 2
Жанр	FPS
Похожесть	Devastation
Мать/отец	Volition,Outrage/THQ
Требует	P3-500(P3-1000), 128(256), 3D
Групповуха	Обломись
Описуха	Порт с PS со всеми вытекающими последствиями. Графика реализована точно под требования PS2, так что красивые навороченные спецэффекты тебе будут только сниться. Сюжет вообще, скорее всего, написан психами, случайно сбежавшими из соответствующего лечебного заведения, ибо разобраться в нем невозможно. Да и вообще вся игра, даже при всем к ней отвращении, проходится за один вечер.
ПРИГОВОР	ЛАЖА





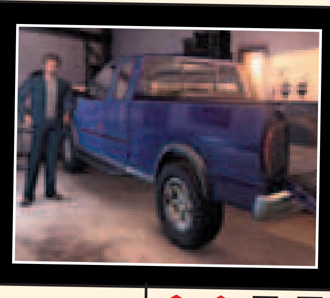
Урожденная	Падал прошлогодний снег
Жанр	Adventure
Похожесть	Дача кота Леопольда
Мать/отец	1С/1С
Требует	P200(P2-350), 32(64)
Групповуха	Обломись
Описуха	Средненькая адвенчура от отечественного производителя, поставленная по сценарию одноименного мультика. Соответствующая игровая атмосфера передана бесподобно, благо графическая и звуковая часть игры заслуживают самых высоких похвал. Но загадки чересчур простые, юмора мало, да и играть не особо интересно. Уж очень не хватает действительно веселых и заводных моментов.
ПРИГОВОР	СРЕДНЕ

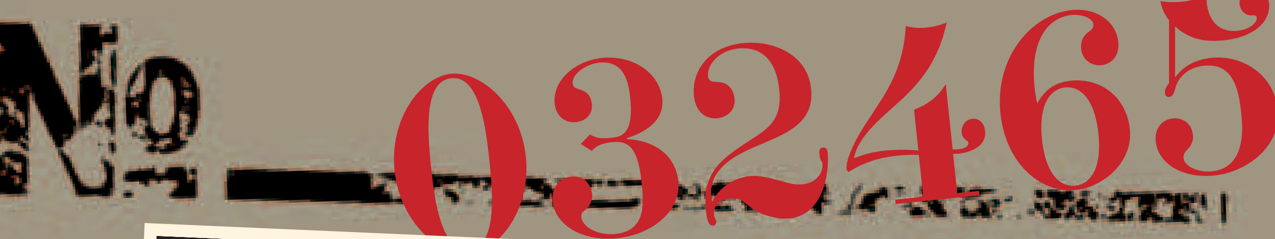




Урожденная	CSI: Crime Scene Investigation
Жанр	Adventure
Похожесть	Pursuit of Justice
Мать/отец	369 Interactive/Ubi Soft
Требует	P2-300(P3-500), 128(256), 3D
Групповуха	Обломись
Описуха	Прямо скажу, не слишком удачная адвенчура, которая, пожалуй, заинтересует лишь фанатов одноименного американского сериала. Видеодвижок не блещет новизной, а звуковое сопровождение и озвученные реплики героев заслуживают самой низкой оценки. Зато сюжет, состоящий из пяти преступлений, которые тебе придется раскрыть, интересен и логичен. Так что игра исключительно на любителя.
ПРИГОВОР	СРЕДНЕ

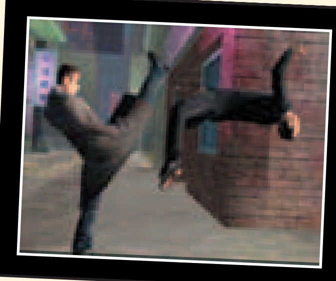








Урожденная	Enter The Matrix
Жанр	TPS + гонки
Похожесть	Max Payne
Мать/отец	Shiny Entertainment/Atari
Требует	P3-800(P4-1500), 128(256), 3D
Групповуха	Обломись
Описуха	Очередной пример того, как разработчики использует раскрученный бренд, выпуская на рынок откровенную лажу. Думаешь, ты сможешь почувствовать себя небезызвестным Нео? Как бы не так, нам предлагают пройти кампании за трех второстепенных героев, появившихся во второй части фильма. Да все бы ничего: и бои на уровне, и погони захватывающие, и саундтреки заводят. Но графика на уровне трехлетней давности.
ПРИГОВОР	СРЕДНЕ





Урожденная	Hot Wheels Bash Arena
Жанр	Аркадные гонки
Похожесть	Серия Hot Wheels
Мать/отец	Micro Forte/THQ
Требует	P233(P2-400), 64(128), 3D
Групповуха	LAN, инет
Описуха	Игрушка из серии "веселая фигня, от которой сложно оторваться". Огромное количество разнообразных машин, несколько десятков трасс (каждая со своими особенностями) и смышленый AI оставляют лишь приятное впечатление от игры. Но с другой стороны - графический движок мог бы быть и получше, а звуки поразнообразнее. Рекомендую только после тяжелого рабочего дня.
ПРИГОВОР	СРЕДНЕ



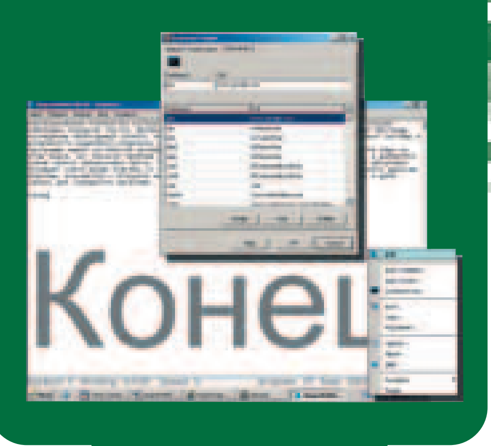


M.J.Ash (m.j.ash@real.xakep.ru)

Assistant Typist v 2.0

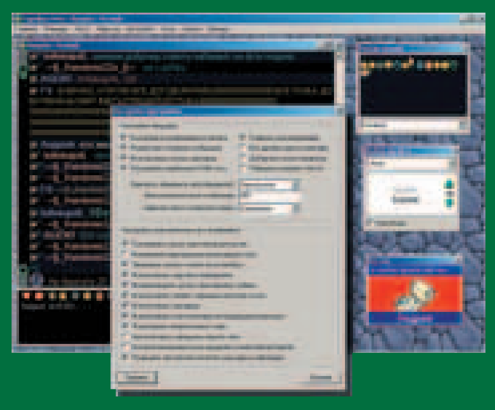
Windows 9x/Me/NT/2k/XP
Size: 529 Kb
Shareware
http://www.smartgesture.com

Сколько понаделано клавиатурных тренажеров для обучения слепому десятипальцевому методу печати, а все без толку. Большинство юзеров при наборе текста по-прежнему не отрывают глаз от клавиатуры. Потычут в клаву двумя пальцами - посмотрят на экран - исправят опечатки. Потычут - посмотрят - исправят... Мучаются страшно, но переучиваться никто не хочет - привыкли уже.
Оригинальную попытку облегчить жизнь таких вот упрямцев предприняли ребята из SmartGesture Lab. Они написали Assistant Typist - программу, позволяющую контролировать периферийным зрением правильность набора текста. Для этого все, что ты печатаешь, Assistant Typist дублирует в нижней части экрана шрифтом очень большого размера. То есть ты можешь долбить по клавишам как обычно, но через какое-то время (если подвинуть клаву поближе к монитору и подобрать в Assistant Typist оптимальные габариты букв) ты невольно начнешь краем глаза читать все, что пишешь. Количество опечаток в твоих текстах тут же радикально уменьшится. Если, конечно, ты до этого времени не окосеешь :).
Помимо этого Assistant Typist предлагает своим пользователям еще три интересные фишечки: автоматическое исправление типичных ошибок, автозамену сокращений и командную строку. Что такое исправление ошибок и опечаток объяснять не буду. Автозамена сокращений - это когда, допустим, твое невыразительное "да?" программа самостоятельно преобразует в вежливое "Ладно, приятель! Давай, выкладывай, что у тебя за проблема". Самой необычной является функция Comand Line. Она обеспечивает выполнение требуемой команды при введении заранее заданного ключевого слова. Не веришь - проверь. Установи Assistant Typist, напечатай где угодно "calc" - запустится калькулятор, набери "goo" - и твоя бродилка мигом забросит тебя на www.google.com.



Капеллан C5 NATIVA

Windows 9x/Me/NT/2k/XP
Size: 3125 Kb
Freeware
http://www.capellan.ru

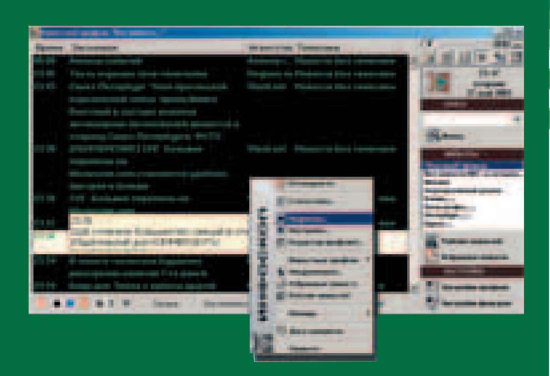


Симпатичный, навороченный, быстрый и нетребовательный к ресурсам чат-браузер, поддерживающий многие популярные системы чатов (такие как "Кроватка", "Чат-Сити", "Фрегат", "Психологический чат" и др.). На редкость любопытная софтина. Для нее любой чат - это лишь механизм обмена информацией. Используя этот механизм, Капеллан передает и принимает сообщения других участников чата. А то, как этот механизм оформлен (дизайн веб-страниц, элементы навигации, баннеры и прочее) программу не интересует. Это остается за бортом - Капеллан использует свои собственные, весьма развитые методы представления информации. Другими словами, любой чат в этом браузере выглядит так, как того хочет пользователь. Побочный эффект такого подхода - набор доступных юзеру фишечек не зависит от того, в каком чате он находится. Защитные фильтры (на мат, флуд), единый для всех чатов игнор-лист, автоматическое уведомление о появлении в чате друзей, кнопки шаблонных фраз и многие другие функции пользователю Капеллан доступны всегда, даже если он тусуется в каком-нибудь примитивном гадюшнике.
Программа может работать в многооконном режиме. Старые сообщения не затираются - ты всегда можешь прокрутить в окне любую дискуссию и даже сохранить ее в виде HTML-файла.
Подключение новых чатов к системе Капеллан осуществляется с помощью специальной библиотеки Chat Linker SDK, доступной в исходных текстах. Однако знакомства с ней тебе, скорей всего, удастся избежать - как я уже говорил, для многих популярных чатов разработчиками уже написаны и выложены на сайте программы все необходимые "драйверы".



Инфоскоп v 1.7

Windows 9x/Me/NT/2k/XP
Size: 1330 Kb
Freeware
http://www.iscope.ru



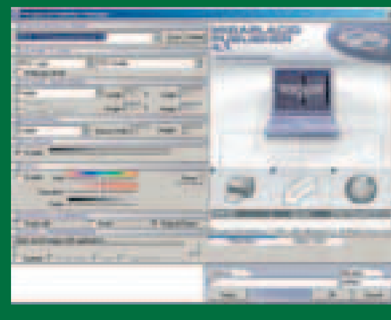
Система получения новостей из разных информационных источников в едином формате. На момент тестирования Инфоскоп уже умел перекачивать на компьютер свежие сообщения из десятка солидных СМИ, таких как Lenta.ru, Compulenta.ru, РИА "Новости" и многих других. Основной смысл существования подобного рода систем заключается в автоматической фильтрации новостных потоков. Инфоскоп не является исключением из правил. Поэтому при настройке программы имеет смысл подписаться лишь на те ленты новостей, которые ты читаешь, а систему фильтров настроить так, чтобы в окне программы отображались сообщения только той тематики, которая тебя интересует.
Помимо удобного просмотра сообщений, система Инфоскоп позволяет распечатывать особенно любопытные или важные заметки, сохранять их на потом или отсылать по электронной почте. Еще одна интересная опция системы - "рейтинг новостей". С его помощью можно отобрать наиболее читаемые пользователями системы новости. Рейтинг строится по количеству прочтений, и первой в списке будет стоять та новость, на которую обратило внимание наибольшее количество пользователей. Также Инфоскоп может похвастаться функцией полнотекстового поиска и механизмом уведомления о поступлении новой инфы.





Miraplacid Publisher v 4.1

Windows 9x/Me/NT/2k/XP
Size: 2107 Kb
Shareware
http://www.miraplacid.com

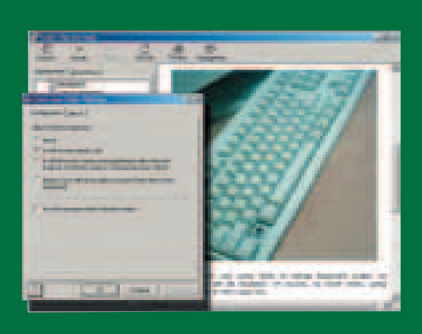


Miraplacid Publisher занимается конвертированием документов в изображения форматов JPEG, TIFF, BMP, PNG или TGA. Программа добавляет новый принтер в систему, и для преобразования документа необходимо его на этом самом принтере просто взять и распечатать. От тебя ускользает смысл подобного преобразования? О, на самом деле необходимость в нем возникает часто! Например, тебе нужно передать какой-нибудь документ (допустим, сверстанную страницу журнала :)) кому-то, у кого на машине нет программы, в которой его можно посмотреть. А обычный графический файл без проблем открывается на любой машине с любым ПО (да и весить этот файл, вполне вероятно, будет меньше, чем исходный документ в оригинальном формате). Еще вариант: защита контента (править или таскать тексты из документа в формате JPEG хотя и возможно, но довольно затруднительно). Кроме того, Miraplacid Publisher можно использовать для дополнительной обработки документов, выводимых на обычный принтер (управление качеством, цветовой гаммой, масштабом, расположением на листе и т.п.).
О степени навороченности программы я, пожалуй, распространяться не буду - имхо, о ней нетрудно догадаться, просто взглянув на прилагаемый скриншот.



I Hate This Key v 1.1

Windows 9x/Me/NT/2k/XP
Size: 492 Kb
Freeware
http://www.bytegems.com



Сейчас трудно встретить клавиатуру, на которой бы не было специальной кнопки с логотипом Windows - Windows Logo. Посмотри на свою клаву - видишь, слева эта зараза втиснулась между клавишами Ctrl и Alt, да еще и продублировала себя справа от клавиши пробела и правого Alt. Необычное расположение, правда? Ей бы сидеть где-нибудь в сторонке, а она наоборот - так и лезет под пальцы. При работе в оконном режиме с офисными приложениями ошибочное нажатие на Windows Logo приводит к появлению на экране меню кнопки Пуск - всего-навсего. Но если по ошибке ткнуть Windows Logo во время игры в Quake или Counter Strike, то ты уже так легко не отделаешься. Скорей всего твоя игрушка мигом выпадет из полноэкранного режима, вернуться в который без перезапуска программы тебе, возможно, и не удастся. В любом случае, крайне ценное время будет потеряно... Именно поэтому клавишу Windows Logo ненавидят геймеры всего мира. Некоторые даже выламывают ее из клавы. Честно говоря, я тоже об этом подумывал. Но потом, к счастью, нашел утилиту I Hate This Key, позволяющую избежать хирургического вмешательства. Если принять в расчет злобное название, можно подумать, что после своего запуска эта утилита вырубает Windows Logo раз и навсегда. Но на самом деле I Hate This Key поступает круче - она препятствует нормальному функционированию Windows Logo лишь тогда, когда ты вздумаешь поиграть. В остальное время эта кнопка работает как обычно. Впрочем, что скрывать, классическое "Вкл./Выкл." в настройках I Hate This Key также предусмотрено.



ШароWAREZ

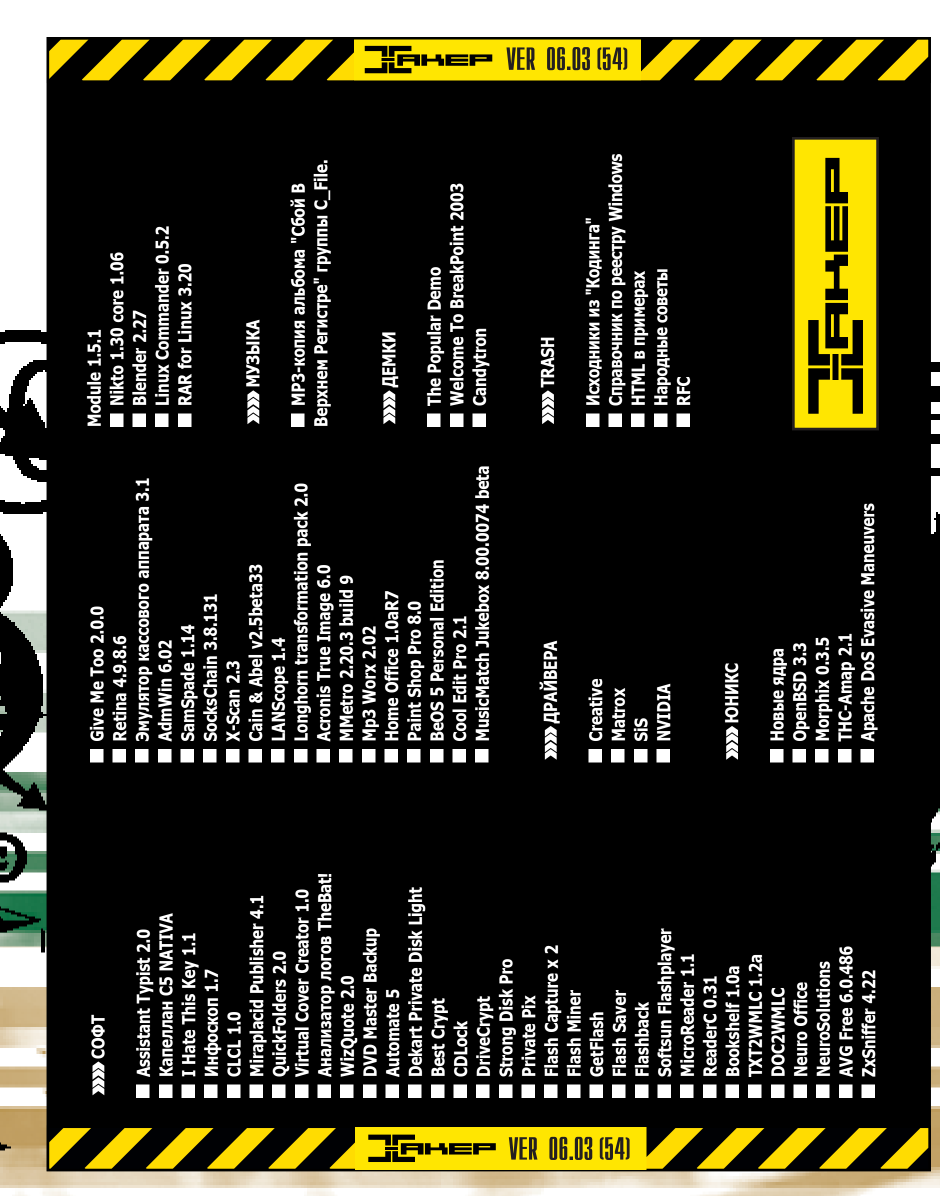
M.J.Ash (www.xknows.com, m.j.ash@real.xakep.ru)

Virtual Cover Creator v 1.0

Windows 9x/Me/NT/2k/XP
Size: 2577 Kb
Shareware
http://www.virtual-cover-creator.net

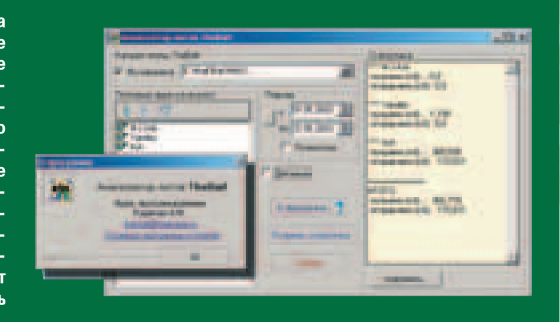
Инструмент для создания трехмерных изображений книг, журналов, папок, блокнотов и коробок (в том числе и коробок для компакт-дисков). С помощью Virtual Cover Creator можно запросто смоделировать "фотографию" упаковки продукта, которого еще нет в продаже. Скажем, слепил ты на коленке прогу - сразу же покажи на своем сайте, как солидно выглядит ее боксовая версия. Аналогичные махинации можно проделывать с ненаписанными романами и невыпущенными CD.
Virtual Cover Creator - софт довольно гибкий. Юзеру предлагается несколько моделей объектов и более сотни готовых вариантов оформления. Само собой, на любую сторону модели ты можешь нанести необходимый текст и натянуть свои собственные картинки. В программу даже встроен графический редактор, хотя пользы от него никакой - очень уж он простенький. Зато к модулю визуализации у меня никаких претензий: он позволяет рассматривать готовый объект со всех сторон, приближаться/удаляться, управлять расположением и яркостью источника освещения, а также прозрачностью теней. Готовое изображение сглаживается для пущей правдоподобности и записывается Virtual Cover Creator'ом в виде JPEG, TIFF, BMP, PNG или GIF-файла.





Анализатор логов The Bat!

Windows 9x/Me/NT/2k/XP
Size: 283 Kb
Freeware
http://www.argyment.ru/fmt/index.htm

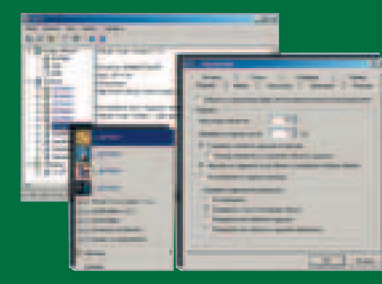


Программа предназначена для анализа логов популярного почтового клиента The Bat! и вывода информации об объеме принятой и отправленной почты за определенный период, как по отдельным почтовым ящикам, так и в сумме. Особенно серьезно относиться к полученной информации не стоит - Анализатор логов не показывает в полной мере объем почтового трафика, он сообщает только мнение The Bat! по этому поводу. Тем не менее, если у тебя нет более точного средства учета (а его у тебя, скорее всего, нет :)), то эта программа может представлять для тебя интерес. Любопытно ведь, сколько килобайт (мегабайт?) весит твоя переписка за месяц (неделю, день, с такого-то по такое-то...). Работает Анализатор логов без установки. Местонахождение почтового каталога узнает из реестра. Или, если стоит соответствующая галочка, лезет в каталог, указанный пользователем. Далее в подкаталогах этого каталога программа ищет файлы account.log, которые затем и анализирует.



CLCL v 1.0

Windows 9x/Me/NT/2k/XP
Size: 140 Kb
Freeware
http://www.nakka.com/soft/clcl/index_rus.html

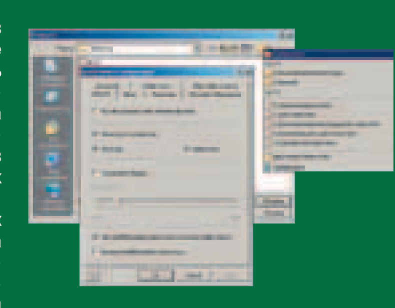


Миниатюрный расширитель возможностей стандартного буфера обмена. Глаза не мозолит, денег не просит, запрограммирован грамотно. Все данные, попадающие в clipboard, CLCL старательно сохраняет в своей базе данных, по умолчанию запоминая последние 30 объектов. При нажатии Alt+C программа выдает их список на экран, позволяя выбрать нужное из меню. Радует глаз продуманность и внешняя простота. Базовый набор функций "вшит" в программу, дополнительные фишечки обеспечиваются плагинами. Кстати, нет необходимости подключать их все - можно выбрать лишь те, которые тебе действительно необходимы. Имеется фильтр форматов - настрой его, и CLCL будет "запоминать" только текст или, скажем, только рисунки. Механизм горячих клавиш внушает уважение: все клавиши можно переназначить, кроме того, ничего не стоит сделать так, чтобы в одном приложении работали одни комбинации, а в другом - другие. Это что касается простоты :). О продуманности же программы говорит хотя бы тот факт, что меню с перечнем сохраненных объектов выпадает по горячей клавише именно там, где у тебя находится курсор мыши! Казалось бы мелочь, а приятно. Да, обрати внимание на скриншот - видишь, в указанном меню присутствуют не только начальные строки сохраненных программой текстов, но и уменьшенные копии "кешированных" ею изображений.

P.S. А еще CLCL поддерживает настраиваемые шаблоны, т.е. ты можешь "забить" в программу шаблоны часто используемых фраз и закрепить за каждым из них горячую клавишу быстрой вставки.

QuickFolders v 2.0

Windows 9x/Me/NT/2k/XP
Size: 1068 Kb
Shareware
http://www.bytegems.com



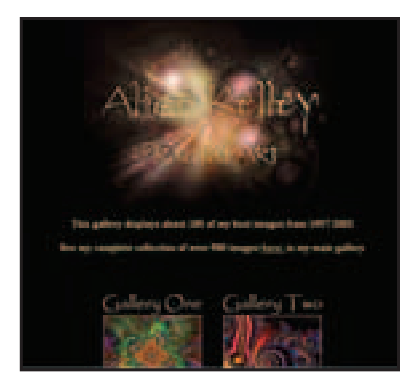
Quick Folders вставляет в стандартные диалоговые окна открыть/сохранить свою кнопочку со звездочкой на морде. Нажатие на эту кнопку вызывает появление на экране меню, в котором находится список часто используемых папок, список недавно открытых файлов (оба этих списка обновляются автоматически) и список твоих любимых папок (который ты формируешь вручную). Клик по нужному элементу любого из этих списков позволяет мгновенно переместиться и сохранить, скажем, текст из Notepad'а в том же каталоге, из которого ты недавно Photoshop'ом открывал картинку. Однако QuickFolders не только облегчает навигацию по файлам и каталогам. Начиная с Windows 2000, в стандартных окнах Open File dialog появился новый элемент - панель адресов (Places bar), служащая для быстрого выбора наиболее популярных и важных (с точки зрения Microsoft) папок, как-то: Журнал, Мои документы, Рабочий стол и т.д. Одна беда - эту подборку иконок никак нельзя назвать удачной. Но с помощью QuickFolders этот недостаток можно легко исправить... Есть у QuickFolders и другие таланты. Например, эта программа умеет монтировать виртуальный диск из указанного каталога и способна подчеркивать важность той или иной папки путем замены их стандартного ярлычка альтернативной картинкой в ico формате.

WWW

Алекс Экслер (exler@exler.ru)

Какие симпатичные фрактальчики

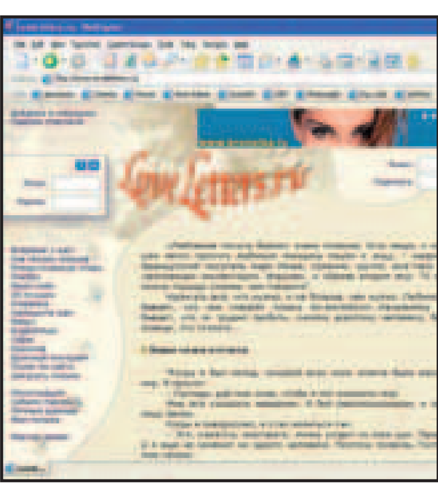
www.alicekelly.com



Видел когда-нибудь всякие разные классные фрактальчики? Что, не знаешь, что такое фрактальчики? Да наверняка знаешь. Потому что когда тебе показывают какую-нибудь загадочную и завораживающую картинку, описать которую человеческий язык в состоянии разве что выражением "ух ты, круто!" - вот это и есть фрактал. Точнее, картинка, построенная с помощью фракталов. Многие пользователи об этом что-то слышали, и когда им на глаза попадается нечто очень красивое и хаотично-упорядоченное, они тут же говорят с легким оттенком пренебрежения: "А-а-а, фракталы. Знаю-знаю". Однако примерно 90% людей, употребляющих термин фрактал, понятия не имеют, что, собственно, он означает. Хочешь, расскажу? Фракталы - это такая стройная математическая и геометрическая теория, позволяющая получить всякие красивые штучки-дрючки. Что? Не нравится объяснение? Ну, я, конечно, могу на ста страницах объяснить суть процесса, но тебе оно надо? Лучше развлекайся этим сайтом, где Элис Келли выставляет свои фрактальные работы. Там просто башку сносит, честное слово!

Любовные письма

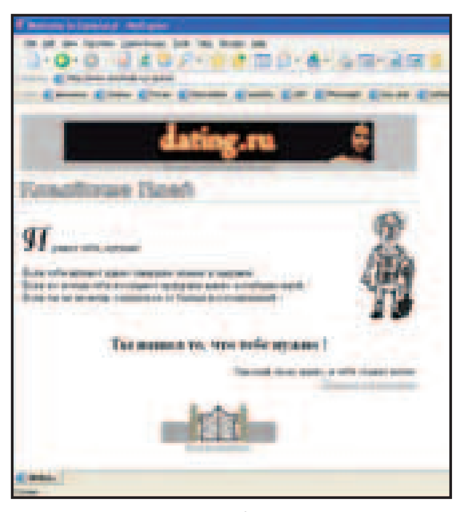
www.loveletters.ru



Что самое интересное, этот сайт - действительно о любовных письмах, а вовсе не так называемая служба знакомств, где профессиональные проститутки хищно косят под гимназисток, а застенчивые школьницы скрывают пыльцу своей невинности под развязным имиджем кабацких шлюх... Нет, нет, и еще раз нет - этот проект не имеет никакого отношения к службе знакомств! Зато на его страницах тебя научат... Да-да, писать любовные письма. Ведь дело это не такое простое, как может показаться на первый взгляд. Составление письма, особенно любовного - дело крайне важное. Его нельзя пускать на самотек, особенно если твое перо не порхает как бабочка и не жалит как оса, а медленно и тягуче ползет по бумаге, высекая искры из натужных деепричастных оборотов, внезапно прорвавшихся сквозь тончайшие капилляры стержня. Вот здесь тебя и научат. И даже, быть может, напишут что-нибудь за тебя. Правда, не знаю, как ты потом будешь выкручиваться при очной ставке, но это уже твои проблемы, ведь так?

Кладбище идей

www.stockmail.ru/~grave

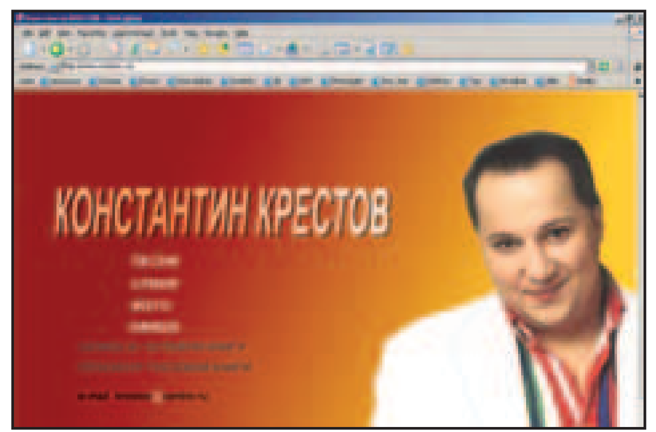


У каждого из нас имеются свои нереализованные идеи. Есть среди них довольно обыденные. Юноши часто лелеют трогательную мысль бросить пить, курить, шляться по барам и накачивать животик пивом. Девушки дают себе страшные клятвы не есть после шести, не употреблять мучного и жирного, а также не носить заштопанные колготки. Но есть идеи менее традиционные и более возвышенные: сдать экзамен, вернуть долги, прекратить играть в покер, убить соседей, перестать слушаться подругу, убраться в комнате или даже вынести из квартиры елку. Все эти идеи слегка отравляют нам существование, потому что никогда не реализуются. Так вот, на этом сайте ты легко можешь похоронить любую мучившую тебя идею, чтобы она навеки ушла и больше никогда не касалась тебя своим укоряющим крылом. Заходишь на сайт, снимаешь шляпу и с почтением выслушиваешь приличествующую случаю музыку Россини и Листа. Затем вступаешь на кладбище, где и начинается процедура погребения... Попробуй! Увидишь, тебе сразу станет легче!

Крестовый поход

www.krestov.ru

Вот ты говоришь: "Дикий интернет, дикий..." Да какой же он дикий? Он фактически домашний! Посмотри, какая милая страничка. Расцветкой - один в один фирма "1С". На обложке - мужик, самодовольный и щекастый. Но загляни внутрь - и хорошее настроение не покинет больше вас (с), однозначно. Просто почитай стихи Константина Крестова, ничего более. Я даже ни одного примера приводить не буду - ты по первой же строчке сам все поймешь. Когда утихнет первая истерика, начинай потихоньку принимать песни Константина, но не больше одной в день, а то врачам потребуется неделя на то, чтобы стереть улыбку с твоего лица. Я рекомендую начать с творения "Последний день весны". На нем же, впрочем, можно и кончиться, если вдруг прослушать этот шедевр целиком. Я такого кошмара не слышал даже на пьяных вечеринках в темно-синем лесу, где щебечут осины и дубы-колдуны. Но комментарии излишни. Ты сам все услышишь.



У посла - медальон

www.earthbounddog.com



Что делать простому потерявшемуся гражданину, когда он не знает, как вернуться домой? Думаешь, такие случаи невозможны - потеря гражданином полной ориентации в пространстве? Разумеется, я не имею в виду случаи, когда эта потеря ориентации носит временный характер и обычно проходит на следующий день, после того как потерявший ориентацию проспится до ее полного восстановления. Я говорю об участившихся слухах о случаях похищения наших сограждан инопланетянами прямо с поверхности Земли. Так вот, что делать в том случае, если тебя похитили инопланетяне и утащили в голубую даль, откуда и Землю-то не разглядеть? Ты помнишь свой номер планеты в тинтуре и номер галактики в спирали? Наверняка не помнишь. Хотя такие вещи должны отскакивать от зубов. Даже если тебя разбудят среди ночи. Даже если рядом с тобой блондинка. Даже если эта блондинка лежит рядом не просто так... Интересно то, что производители медальона - не какие-нибудь шаромыжники. Там даже заявляется, цитирую: "Если вы будете похищены, и при наличии этого медальона не будете доставлены обратно на Землю, мы гарантируем вам возврат полной стоимости покупки".

Среднестатистический фейс Рунета

www.interface.net.ru

Идея интересная - набрать много-много самодельных портретов интернетошатающихся, а затем на их основе сотворить нечто среднестатистическое. Правда, толку с такой средней статистики довольно мало, потому что среднестатистические надбровные дуги и среднестатистические уши мало что скажут уму и сердцу, но любая забава делается для того, чтобы забавляться, а не статизировать, и здесь можно позабавиться со страшной силой. Зайди туда, полюбуйся уже созданными среднестатистическими портретами Рунета - мужским и женским. Мужской напоминает комсомольца с лютым недосыпом после изучения десяти заповедей марксизма, зато женский - миловидная девушка с прической "Бабетта, наплевавшая на парикмахеров", весьма похожая на мою институтскую старосту. Между прочим, в программе усредняется весьма немаленькое количество уже загруженных изображений. На данный момент там 1839 мужских портретов и 1119 женских. Женщины явно пока проигрывают в количестве, но выигрывают в качестве. Впрочем, все зависит от тебя. Зайди и добавь свой портрет.



FAQ

Stepan Ilyin aka Step (faq@real.xakep.ru)

Задавая вопрос, подумай! Не стоит мне посылать вопросы, так или иначе связанные с хаком/кряком/фриком - для этой есть hack-faq (hackfaq@real.xakep.ru), не стоит также задавать откровенно ламерские вопросы, ответ на которые ты при определенном желании можешь найти и сам. Я не телепат, поэтому конкретизируй вопрос, присылай как можно больше информации.

Q: Учу Delphi. Проблема такая: надо из одной программы открыть другое windows-приложение, а потом его же закрыть. Спрашивается, как это можно реализовать?

ответ

A: Реализовать это несложно. Достаточно лишь внимательно прочитать ту часть справки, где описываются способы использования команд WinExec(...), ShellExecute(...), PostMessage(FindWindow(...), WM_CLOSE(...).

Q: Я живу провинции. Почему ни один из трех, работающих здесь провайдеров, не поддерживает протокол V.92?

ответ

A: Дело в том, что многие провайдеры (тем более провинциальные) не поддерживают Up Stream, так как используют пулы, "стоящие" на старых cisco 5300. А для полноценного V.92 нужен как минимум cisco 5350. Могу лишь посоветовать смириться с таким положением дел или переехать в городок покрупнее.

Q: В маленький офис приобрели 2 ноутбука: один - шефу, другой - его секретарше. Задача, в общем-то, простая - соединить эти два компьютера в маленькую сеть. Только вот что-то никак не получается: и то пробовал, и это. Все без толку. На машинах стоит WinXP, сетевые карточки 100Mb. Помогите, пожалуйста: опишите элементарную схему соединения двух компьютеров в сеть.

ответ

A: Соединение в сеть двух ноутбуков принципиально ничем не отличается от аналогичной операции с PC. Как я понял, хаба у тебя нет, следовательно, придется воспользоваться "нуль-хабным" (или "cross-over") кабелем. Достать его несложно, он продается в любом компьютерном магазине, однако при определенном желании (и умении) его можно сделать и самому. Для этого потребуется следующая разводка проводов в разъемах:

1 3 бело-зеленый провод
2 6 зеленый
3 1 бело-оранжевый
4 4 синий
5 5 бело-синий
6 2 оранжевый
7 7 бело-коричневый

После все должно пойти как по маслу. В лучшем случае, WinXP сама настроит сеть. В худшем - тебе придется проделать следующие операции. Для первой машины указать статический IP-адрес 192.168.0.1 и маску подсети 255.255.255.0, для второй - соответственно 192.168.0.2 и 255.255.255.0.

Q: Здравствуйте! Несмотря на то, что город у нас провинциальный, локальных сетей довольно много, причем больших. Например, в нашей сети 27 человек. Неудивительно, что недавно мы решили провести выделенный канал. Уже обо всем договорились, на следующей неделе будут ставить радиомодем. Осталась одна проблема - трафик весьма и весьма дорогой, поэтому нужен четкий контроль, сколько, кто, и когда качает. Так, чтобы в конце месяца каждому был предоставлен денежный счет. Поделитесь опытом!

вопрос

ответ

A: Проблема действительно очень актуальна, но решается довольно просто. Надо лишь найти подходящую биллинговую систему. Из личного опыта могу предложить следующее:

NetUP UserTrafManager (http://www.netup.ru/)
Billing System for ISP (BISP) (http://www.billing.kiev.ua/)
Phonekeeper (http://www.tsoft.ru/)
LANBilling (http://www.lanbilling.ru/)
ABACS (http://www.abacs.ru/)

Есть платные и бесплатные биллинговые системы. Последние, как правило, похуже, поэтому советую скинуться и раскошелиться на что-нибудь коммерческое, но качественное и надежное. Тем более что полагающая система поддержки пользователей будет очень кстати.

Q: У меня стоит Mandrake 7.0 (я столько с ним провозился, что ставить другую, более новую версию просто нет сил). Вроде бы все хорошо, но есть одна проблема. Я не знаю, как уменьшить интервал времени до гашения монитора...

ответ

A: Нет ничего проще! В файл /etc/sysconfig/console/setterm допиши следующее: -blank <количество минут до гашения монитора>. Если значение этого параметра равно "0" - монитор не гаснет совсем.

Q: Почему в последнее время я часто встречаю фразы, типа "Фидо - отстой", "фидорас". Ведь фидо - очень полезная сетка!

вопрос

ответ

A: Действительно, неуклонный рост инета и все большая его доступность (чему X всячески содействует) отодвигают фидо на задний план. Многие люди, приобщившиеся к инету, вспоминают фидо как дела давно минувших дней. Отсюда и такие фразы. Если хочешь знать мое мнение, я с ними не согласен. Да, netmail и рядом не стоит с e-mail'ом, и количество файлов, идущих по файлэхам не может сравниться с терабайтами warez'a в интернете, но есть у фидо один большой ПЛЮС - это эхоконференции. Никакие форумы (за редким исключением) не могут сравниться с фидошными эхами. Их настолько много, что всегда можно найти те, которые тебе по душе, те, где практически всегда можно получить ответ. Так что забей на всех, кто умаляет полезность фидо. Ведь, скорее всего, они эту сеть и не видели. Твой 2:5023/31 :).

Q: Как в windows-based операционных системах узнать mac-адрес компьютера?

вопрос

ответ

A: Windows XP: getmac
Windows 2000: ipconfig /all
Windows 9x: winipconfig

Q: Как, используя PHP, определить валидность URL?

вопрос

ответ

A: Держи кусочек скрипта, который уже давно гуляет по инету и встречается во множестве скриптов:

```
<?
function check_url($url) {
   if (eregi( '^http://', $url)) {
      $urlArray = parse_url($url);
      if (!$urlArray[port]) $urlArray[port] = '80';
      if (!$urlArray[path]) $urlArray[path] = '/';
      $sock = fsockopen($urlArray[host], $urlArray[port], &$errnum,
             &$errstr);
      if (!$sock) $res = 'DNS';
      else {
      $dump .= "GET $urlArray[path] HTTP/1.1\r\n";
      $dump .= "Host: $urlArray[host]\r\nConnection: close\r\n";
      $dump .= "Connection: close\r\n";
      fputs($sock, $dump);
      while ($str = fgets($sock, 1024)) {
         if (eregi("^http/[0-9]+.[0-9]+ ([0-9]{3}) [a-z ]*", $str))
            $res[code] = trim(eregi_replace(
            '^http/[0-9]+.[0-9]+([0-9]{3})[a-z ]*',
            "\\1", $str));
         if (eregi("^Content-Type: ", $str))
            $res[contentType] = trim(eregi_replace(
            "^Content-Type: ", "", $str));
      }
      fclose($sock);
      flush();
      return $res[code];
      }
   } else $res = "N/A";
   return $res;
}
?>
```

Q: По вашей рекомендации купил себе новенький Radeon. Но как мне проверить правильность работы RivaTuner'a, а точнее SoftR9700?

вопрос

ответ

A: Для начала можно проверить дату %windir%\system32\drivers\ati2mtag.sys и ati2mtag.sys, входящего в дистрибутив. Они должны быть разными. Можно поступить и по-другому. Зайди в закладку Display properties -> Adapter -> Adapter information -> Chip type. Здесь должно отображаться "Radeon 9700".

NEXT

«Я ПЛАКАЛ» АКА ЛАМАРАЗМЫ НОМЕРА:

Мы с другом скачали взломщик интернета. Честно говоря, не знаю, как он работает, да и неважно это - главное, чтобы работал! А там предупреждение - мол, юзать надо правильно, следуя всем инструкциям, иначе за последствия разработчики не ручаются. Попробовали у меня, попробовали у друга, но ничего не вышло. Замечу, что все предыдущие действия делали полностью по инструкции. Заперлись вот здесь: "Пункт 13. Итак, почти все готово. Перегружайте и после сообщения "No system disc or disc error" три раза наберите на клавиатуре "fReE iNTeRTet" (соблюдая регистр букв). Вуаля, вы в интернете".
Помогите, никакого инета не появилось, более того, я не могу закрыть эту программу и нормально работать на компьютере. А скоро мама приедет - она иногда очень важные документы редактирует! (у друга та же фигня). Может, БИОС сбросить?

Q: Поставили в офис АДСЛ. Вроде все ничего, пинги неплохие (20-40), бывают, правда, иногда маленькие потери пакетов. Но Бог с ними. Проблема в другом... В программах, использующих udp соединения, постоянно идут потери пакетов, соответственно, и лаги. Например, во всем известную игрушку Counter-Strike играть крайне проблематично. Уже несколько раз обращался к провайдеру - говорят, что проблема где-то у меня. Помогите!

вопрос

ответ

A: Делать выводы без непосредственного осмотра довольно сложно, но смею предположить, что проблема, скорее всего, заключается в следующем. Один или несколько роутеров на пути от тебя до игрового сервера сильно перегружены. Причем в их настройках активизирована функция так называемой "разгрузки". То есть во время затыка роутер либо ставит UDP пакеты в очередь, либо просто их удаляет, чтобы дать пройти TCP пакетам (у которых приоритет, как правило, несколько выше). Отсюда и временные жуткие пинги и потери пакетов. Единственный выход в данном случае - убедить провайдера перенастроить свой роутинг, что сделать непросто, учитывая неоправданную уверенность админов в том, что проблема не в этом.

FAQ

Stepan Ilyin aka Step (faq@real.xakep.ru)

Q: Привет! Я собрался покупать модем, ищу что-нибудь недорогое, но в то же время качественное. Что можешь сказать по поводу модемов Acorp?
A: На российском рынке в основном представлено 3 модели модемов Acorp. Обо всех по порядку:

вопрос

ответ

A: На российском рынке в основном представлено 3 модели модемов Acorp. Обо всех по порядку:
1. Acorp M-56PIM2. Это бесконтроллерный PCI-модем, у которого есть цифровой процессор сигналов (DSP), но нет управляющего контроллера, ПЗУ и буферной памяти. Модем съедает значительную часть ресурсов слабых компьютеров. Тем не менее, кое-как поддерживает V.92 и обеспечивает очень неплохой уровень связи. И что самое главное - стоит всего $20-25. Так что если с деньгами проблема - это, по-моему, наилучший выбор.
2. Acorp M-56EUS. Своеобразный модем. Хотя он и внешний, но относится к классу софтовых модемов. То есть, и этот модем вряд ли подойдет владельцам раритетных машин. Как, впрочем, и всем остальным, потому что хорошее соединение с минимум дисконнектов тебе с этим модемом будет только сниться... ;(
3. Acorp M-56EMSF2. Один из самых популярных внешних модемов. Идеален по соотношению цена/качество, благодаря которому он и завоевал большую армию поклонников. Отличная связь и широкая функциональность выводят его в число лидеров среди модемов этого класса. Хотя качество связи его предшественника, Acorp M-56EMSF, мне совершенно не понравилось...

Q: У меня уже давно есть сайт, движок которого полностью написан мною на PHP... Ссылки выглядят так: www.muziki.net/mp3/rusian.php?page=1. Спрашивается: как сделать так, чтобы эта же ссылка выглядела так: www.muziki.net/mp3/1? Помню, что это можно сделать автоматически, используя настройки сервера, но никак не могу вспомнить как...

вопрос

ответ

A: Делается это элементарно. Открой на сервере .htaccess и добавь следующее:

```
RewriteEngine On
RewriteRule ^mp3(\d*) /mp3/russian.php?page=($1)
```

Q: Спасибо вам за ответы по PHP. Они здорово помогают. Я пишу веб-сервер обмена файлами, и у меня появился такой вопрос: как можно составить список всех файлов в директории и записать их в массив?

вопрос

ответ

A: Например, так:

```
if ($handle = opendir('.'))
 {
  while (false !== ($file = readdir($handle)))
   {
    if (is_dir($file)) continue;
    $f_arr[] = $file;
   }
  closedir($handle);
  print_r($f_arr);
 }
else print 'error';
?>
```

Q: А каким образом на perl'е можно проверить правильность e-mail адреса?

вопрос

ответ

A: На мой взгляд, рациональнее всего это можно сделать так:

```
 if (!preg_match("/^(.+)@[a-zA-Z0-9-]+\.[a-zA-Z0-9.-]+$/si", $email)) {
   echo "ОШИБКА! НЕВЕРНЫЙ E-MAIL!!!";
 }
```

Q: Пожалуйста, подскажите! Я решил взять материнку ASUS P4PE, но в магазине их две: одна с LAN, другая с LAN, FireWire и SerialATA. А разница в цене весьма существенная (особенно для моего кармана). Отсюда вопрос: стоит ли брать ту вариацию, которая комплектуется SeialATA, или игра не стоит свеч?

вопрос

ответ

A: Я почти уверен, что винчестера, поддерживающего SerialATA, у тебя нет. Ведь так? Зачем же тогда брать материнскую плату с поддержкой этого стандарта? Тем более что прирост производительности от SerialATA ничтожно низок. Более того, до поддерживаемой Serial ATA скорости чтения с пластин 150MB/сек производителям винчестеров еще о-о-очень далеко. Так далеко, что ты за это время еще не раз поменяешь материнку. Замечу, что Asus P4PE на данный момент - не самый лучший выбор. Ведь чипсет i845PE уже давно не новинка. Куда рациональнее (с точки зрения будущего апргейда) взять материнскую плату на чипсете i865PE или, еще лучше, i875PE. Здесь и Serial ATA, и AGP 8X, и двухканальные DDR, и шустрая шина, и немало других менее известных, но весьма полезных наворотов.

Q: Так получилось, что у меня нет полноценного доступа к интернету. Зато в пользовании e-mail'ом я не ограничен, поэтому постоянно пользуюсь услугами сервисов, которые присылают ВВВ-странички мне в ящик. Но каждый раз писать запросы вручную откровенно парит, может быть, подскажешь софт для автоматизации этой рутинной работы?

вопрос

ответ

A: Когда-то тоже сталкивался с такой проблемой. К счастью, это в прошлом. Тем не менее, держи ссылки на подходящий софт:
SuperMail 1.6 (259kb, FreeWare), http://mailweb.r2.ru/click/count.php?go=5
Qbem 2.0 (429kb, FreeWare), http://www.dxfania.boom.ru
Power2Mail v 3.03 (557Kb, ShareWare), http://power2mail.narod.ru
iSnoobyFileByEMail (133Kb, ShareWare), www.filebyemail.narod.ru
FileByEmail 1.0 (327Kb, ShareWare), ftp.mgul.ac.ru/pub/Win/Network/Internet/filebyemail_ver1_0_setup.exe

Q: Можно ли перегнать потоковое видео (asf) в mpeg4?

вопрос

ответ

A: Разумеется. По-моему, самый простой способ - воспользоваться программой mencoder (ftp://ftp.mplayerhq.hu/MPlayer/releases/). Понять принцип ее работы сможет и младенец, поэтому подробно рассказывать не буду.



Р Е Д А К Ц И О Н Н А Я

ПОДПИСКА!

ВЫ МОЖЕТЕ ОФОРМИТЬ РЕДАКЦИОННУЮ ПОДПИСКУ НА ЛЮБОЙ РОССИЙСКИЙ АДРЕС

ДЛЯ ЭТОГО НЕОБХОДИМО:

1. Заполнить подписной купон (или его ксерокопию)

2. Заполнить квитанцию (или ксерокопию). Стоимость подписки заполняется из расчета:

Хакер
6 месяцев - 480 рублей
12 месяцев - 960 рублей

Хакер+CD
6 месяцев - 660 рублей
12 месяцев - 1320 рублей
(В стоимость подписки включена доставка заказной бандеролью.)

3. Перечислить стоимость подписки через сбербанк.

4. Обязательно прислать в редакцию копию оплаченной квитанции с четко заполненным купоном
или по электронной почте subscribe_xa@gameland.ru
или по факсу 924-9694 (с пометкой "редакционная подписка").
или по адресу:
103031, Москва, Дмитровский переулок, д 4, строение 2, ООО "Гейм Лэнд" (с пометкой "Редакционная подписка").

Рекомендуем использовать электронную почту или факс.

ВНИМАНИЕ!

Подписка производится с номера, выходящего через один календарный месяц после оплаты. Например, если вы производите оплату в Сентябре, то подписку можете оформить с Декабря.

СПРАВКИ
по электронной почте
subscribe_xa@gameland.ru
или по тел. (095)292-3908,
292-5463

ПОДПИСНОЙ КУПОН (редакционная подписка)

Прошу оформить подписку на журнал "Хакер"

☐ На 6 месяцев (начиная с ____________ 2003 г.)
☐ На 12 месяцев (начиная с ____________ 2003 г.)
(отметьте квадрат, выбранного варианта подписки)

Ф.И.О. ____________________

Город/село ____________ ул. ____________

Дом ______ корп. ______ кв. ______ тел. ______

Сумма оплаты ____________

Подпись ______ Дата ______ e-mail: ______

Копия платежного поручения прилагается.

Извещение

ИНН 7729410015 ООО"ГеймЛэнд"
ЗАО «Международный Московский Банк», г. Москва
р/с №40702810700010298407
к/с №30101810300000000545
БИК 044525545
Плательщик
Адрес (с индексом)

Назначение платежа	Сумма
Оплата журнала "Хакер" за 200_г.	

Подпись плательщика

Кассир

ИНН 7729410015 ООО"ГеймЛэнд"
ЗАО «Международный Московский Банк», г. Москва
р/с №40702810700010298407
к/с №30101810300000000545
БИК 044525545
Плательщик
Адрес (с индексом)

Назначение платежа	Сумма
Оплата журнала "Хакер" за 200_г.	

Подпись плательщика

Квитанция

Кассир

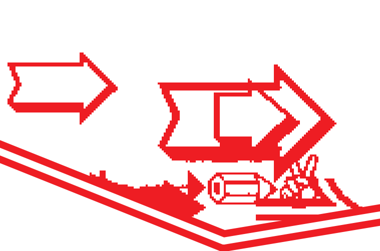
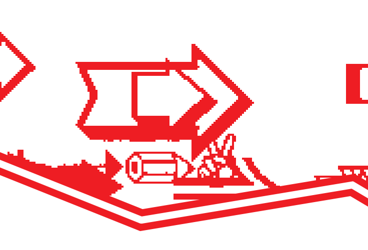
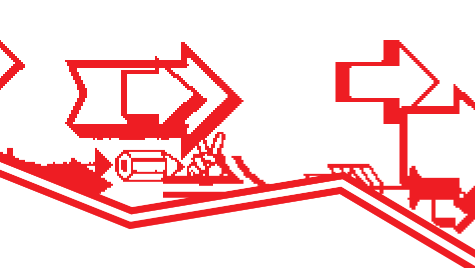
Подписка для юридических лиц

Юридическим лицам для оформления подписки необходимо прислать заявку на получение счета для оплаты по адресу subscribe_si@gameland.ru или по факсу 924-9694 (с пометкой "редакционная подписка"). В заявке указать полные банковские реквизиты и адрес получателя. Подписка оформляется на 12 месяцев, начиная с месяца, следующего после оплаты.

ё-MAIL

Наше е-мыло: magazine@real.xakep.ru

НА ПИСЬМА ОТВЕЧАЛ AVALANCHE

From: Андрей Шишмарев [ashilim@mail.ru]
Subject: n/a

Приветствую Тебя, о Великий][!!!
Я, из племени начинающих (в простонародье "чайники"), пришел к Тебе, о Великий][, с вопросом и маленьким советом. Не откажи в великодушии выслушать меня.
Вопрос у меня такой: при загрузке ОС (Win Me) запускается в "Безопасном режиме". Загружаюсь через F8, вручную запускаю все компоненты - нет проблем. Перезагружаюсь - опять, опа, "Безопасный режим". Что делать?
Теперь маленький совет для X-Puzzle. Посмотрел, почитал я эту рубрику и ничегошеньки не понял. Где же для нашего роду-племени, т.е. "Чайников", чего-нибудь вкусненького? Предлагаю что-то вроде кроссворда, простенько и познавательно. Благодарю Тебя за потраченное на меня время.
Желаю Тебе процветания и удачи!

Правильно, Андрей. Я тоже давно предлагал Ядовитому кроссворд в виде буквы "ХА" публиковать, да чтобы вопросы попроще были. Но он что-то ни в какую. По ходу размышлений на эту тему у меня возникли еще такие идеи: "Х по точкам" - мы напечатаем точки с номерами, первый, кто их по порядку соединит (для усложнения можно числа в восьмеричной системе исчисления писать), прочитает получившееся слово "Хакер" и пришлет нам на мыло отсканированную страницу, получит P4 3.06 GHz. Еще можно лабиринты печатать: нужно будет карандашиком аккуратненько путь изобразить и опять нам прислать. Тут как бонус надо бесплатную путевку в Сибирь давать, чтобы оттуда потом пешком домой топали - учились искать выход из лабиринта. А как тебе идея "бумажная подруга хакера" - печатаем рисованную тетю, и в каждом номере по предмету туалета для нее: кто красивее оденет (или разденет - на что фантазии хватит), тому приз! Круто? Сегодня пойду все начальству рассказывать, может, бонус датут! :)
Про винды твои, кстати, ничего не могу сказать, кроме одного: стирай их на фиг! Ведь даже XP уже три года стукнуло! Microsoft недавно Windows 2003 Server зарелизила (надо будет его как следует опробовать). Как можно до сих пор пользоваться этим убожеством - виндами 9х (программеры меня поймут)? И пусть мне кинет свой своп по мылу первый, кто найдет современную игру, которая не работает под XP! Да что там игры, новый офис (выйдет осенью) только на NT-системах будет функциклировать.
Вы все еще кипятитесь с Win 9x? Тогда мы идем к вам! :)



From: Игорь Ким [kim_igor@bk.ru]
Subject: Хакер ХОЙ!!!

Согласен я со многими, что журнал - cool! Не буду говорить, что я его читаю уже полгода, а буду критиковать за все!!! К журналу с трудом, вроде, можно придраться... Правда, вот почему у вас РЕДКО появляется BugTraq? :(И когда вы отправляете письма в ламаразмы номера, НЕ ОТВЕЧАЕТЕ на них??!!!

Насчет сайта - КУЧА вопросов:
1) Какого у вас с мыла письма не отправляются (например, пишет qmail-inject: fatal: qq write error or disk full (#4.3.0), у меня мыльник Rock_Forever@xakep.ru)
2) Когда наладите с SMTP?
3) Вы никогда не отвечаете на Hack-FAQ (я 3-4 раза вам писал)!!!
4) Если на диске нет крэков для прог, хотя бы уж на них ссылки бы дали... Или даже на сайте поставили.

Хелов, Игорь! Отвечаю на твои вопросы по порядку.

1-2. Ярким пламенем горит надпись "Вопросы" в разделе "ПОЧТА" на сайте www.xakep.ru. Нажимаем - попадаем на http://www1.xakep.ru/post/18323/default.asp.
3. Отвечаем. Регулярно. (Смотри "HACK-FAQ" во "ВЗЛОМе".)
4. Название журнала не означает, что его делают уголовники. Мы еще слишком молоды, чтобы небо в клеточку созерцать :). И вообще, Х никогда не пропагандировал использование пиратского софта. Мы, наоборот, призываем всех пользоваться только лицензионными программами. Интересно, почему все по-другому думают? :)

P.S. Читай журнал повнимательнее (или регулярнее): Bugtraq'a уже полгода как след пропал, на Д-письма же мы всегда отвечаем. В журнале. (См. рядом.)



From: Blauengel [goleva@volgodon.ru]
Subject: Крик души...

Привет, "Хацкер"!!! Я тебя читаю не так давно, также как и увлекаюсь компами. Я узнала о твоем существовании от своего парня (ярого компутерщика:)) и с тех пор стараюсь не пропустить ни одного номера. Журнал мне нравится: прикольный, много полезной инфы и т.д. и т.п. Но меня смущает всегда тот факт, что журнал написан только для представителей мужского пола. Ну а типа девчонки все - тупые блондинки (обыднооо), увлекаются только... да чем они, вообще, увлекаются??? Смотрят моду, картинки в "Космополитене" (или как он там?), а компы для них - набор пимпочек, непонятных железочек и, вообще, это вещь ненужная. Я, конечно, не говорю, что я - просто хацкер`ша. Ессесно, пару раз винду переустановила, и это ничего не значит. Но ведь наша жизнь - постепенное совершенствование. Я считаю, что каждый человек вправе заниматься тем, что ему интересно. И не очень бывает приятно, когда в журнале к тебе обращаются: "Привет, парень! Знаешь, как подцепить красотку?" Да, в вашем творении таких обращений полно. Но ведь Домострой давно на том свете отдыхает. Вот и пусть спит. А вы должны учитывать, что представительницам женского пола тоже интересно увлекаться компами, узнавать много инфы о прогрессе, пить пиво, ломать проги и сети, юзать халявный инет, играть в кровавые кваки и т.д. и т.п. Конечно, такая несправедливость исходит не только от вас. Вы даже можете не читать мое письмо, удалить его просто автоматически... Но зачем о других несправедливостях? Вы кульные. Уж звиняйте за наезды, но я же от чистого стучащего органа :). Ну, и хотелось бы, чтобы вы давали много инфы и для юзверей, а не только для продвинутых программеров.
З.Ы. Давайте жить дружно :-).

Очень приятно получать такие письма. Все равно, что девушки пишут, - лишь бы писали :). Не менее любопытно было узнать, что "представительницам женского пола" тоже интересно играть в кровавые игры. Я, честно говоря, за подобными занятиями их пока не встречал (но зрелище, наверное, неслабое).
А на самом деле мы девушек любим и ни в коей мере не хотим их обижать. Но согласись, подруга, если бы мы написали: "Привет, девчонка! Знаешь, как подцепить красотку?" - это было бы несколько странно. Или нужно так: "Привет, красотка! Хочешь подцепить отличного мужика?" Гм. Можно, конечно, попробовать. Но что-то меня терзают сомненья по поводу ласкового содержания ответных писем от большинства наших читателей-парней.



From: verba_p@rambler.ru
Subject: ...Important subject...

Здравствуйте, уважаемая редакция журнала "Хакер". Я ваш постоянный читатель. Наконец-то решил вам написать. Ответьте мне, пожалуйста, на один вопрос: я скачал интернет, что мне теперь с ним делать?
С уважением, Павел Верба

Будь здоров, Павел. Извиняй, сегодня не твой день. Твое законное место занял Юрец Фролофф со своим фрезеровальным станком. Еще что-нибудь в духе "мама, у меня в твой порт AGP выделенка не включается" придумаешь, пиши.

From: cool_alien [c-alien@yandex.ru]
Subject: e-mail

Здароф, братки! Начну с критики.
Какого, спрашивается,][рена в вашем журнале так мало страниц? Надеюсь, в ближайшем будущем исправитесь. Еще меня не устраивает то, что нет рубрик типа "Вирусы" (чтоб новости про всякие, типа, вири и про какой новый появился, как действует и как с ним бороться). И еще бы побольше про кряк (это, блин, интересно иногда бывает).][отя, может, про это у вас уже есть, я, к сожалению, давно не читал ваш журнал :(. Просто я где-то с октября 2002 г. пропадал (не помню где, но последнее, что помню, - купил гейму "Ядерный Титбит", дальше как в тумане). Вот, вроде, и все!
Напоследок, никак не могу понять: в чем разница между лилипутом и карликом, почему супермен носит плавки поверх всего, и куда делся агент Малдер. Если знаете ответ, напишите, буду, типа, рад и все такое.
Ну все, format, как говорится, C:.

Йоу, братан!
Спешу тебя разочаровать: новостей про новые вирусы нет, ввиду того, что новых вирусов нет как таковых. Все, что мы сейчас наблюдаем, - это разгул червей (но не вирусов в первоначальном значении этого слова). Масштаб поражения зависит от профессионализма автора данного экземпляра и выбранного им способа распространения своего создания. Тут, в общем-то, ничего интересного нет, так как в принципе вся эта гадость очень похожа.

From: Yura Froloff [madhedgehog49@mail.ru]
Subject: n\a

Здравствуйте][aker'ы, у меня возникла проблемка. Подключил я значит фрезерный станок с ЧПУ к ПК, но выньдос не обнаружил его, посоветуйте, что мне делать. Может, в суд подать на мелкомягких за то, что они дров не накатали на станки, или другой выход есть?
Заранее спасибо.
MadHedgehog49@mail.ru

Наивная попытка получить значок "Д". Что ж, я тоже прикинусь паровозом :).

ХУМОР

orginal version: Андрей Глуховцев
<gzoor@mail.ru>
funky edition: Даниил Шеповалов



БУРАТИНО "2003

Пробуждение было жестоким. Папа Карло с трудом оторвал свое бренное тело от заплеванного пола и принял устойчивое положение на четырех точках. Голова, похоже, имела форму чемодана и жутко болела, как будто в ней работал отбойный молоток. Любое движение вызывало приступы рвоты. Стоя на четвереньках, Карло отчаянно боролся с земным притяжением.
- Карло, - проревел в уши чей-то голос.
- М-м-м, - начал, было, Карло, и в это время его стошнило.
- Карло! Что ты вчера спьяну смастерил? - спросил Джузеппе, с грустью разглядывая испачканные брюки.
- М-м-м, где? - неохотно поинтересовался Карло. Джузеппе показал грязным пальцем в сторону грубо сколоченного стола. На столе лежало нечто громоздкое, покрытое простыней. Из-под простыни, отливая металлом, торчали кривые ноги, обутые в грубые кирзовые сапоги 75-го размера.
- А-а-а, это мой сынок, Буратино, - пробулькал, нежно улыбаясь, папа Карло.
Ноги под простыней задергались. Затем из-под простыни появилась кривая рука. Резким движением она сорвала грязное покрывало. Изумленному взгляду собутыльников предстало творение папы Карло. Это была уродливая пародия на человека, метра два с половиной ростом. Из бочкообразного тела торчали пять, нет, даже шесть конечностей. Две руки, две ноги, шарообразная голова с маленькими красными глазками, на которую было натянуто что-то похожее на чехол от обтекателя ракеты среднего размера, любовно окрашенный красными и белыми полосками. Шестая конечность имела вид огромного водопроводного крана, нахально торчавшего чуть ниже живота. Внезапно в недрах туловища что-то забулькало и заклокотало. Из крана повисла большая мутная капля.
- Ты бы хоть оделся, сынок, - произнес папа Карло. Его глаза светились любовью.

- Засохни, плесень, - презрительно ответил Буратино. После чего сделал несколько твердых шагов к полуразрушенному шкафу, из недр которого торчала ручка шарманки папы Карло. Гнилые доски пола под тяжелыми шагами Буратино обращались в прах. В разные стороны разбегались насекомые, лишившиеся своего убежища.
Папу Карло опять начал долбить сушняк. Он ползал по полу в поисках какой-нибудь жидкости. Похоже, что труха и полчища насекомых, решивших поменять место дислокации, его вовсе не волновали. Между тем Буратино, вооружившись инструментами, начал ковыряться в потрохах шарманки. Через некоторое время, удовлетворенно хмыкнув, он закончил свою работу и смел под стол лишние детали. В этот момент из какой-то щели выпал обдолбленный сверчок. Блаженно улыбаясь и путаясь в конечностях, он обратил свой затуманенный взор на Буратино. Разобравшись в своих руках-ногах и приведя их в порядок, сверчок обратился к деревянному уроду с менторской речью:
- Буратино, что ты сделал с шарманкой папы Карло? Зачем ты сломал ее?
Повисла неловкая пауза.
- Шел бы лучше в школу уму-разуму набираться, - продолжал елейным голосом сверчок. Глаза Буратино засветились недобрым красным светом. Он вскинул шарманку и несколько раз крутанул ручку. Шарманка, громко завизжав, раскрутила стволы и начала посылать смертоносные снаряды в цель. Ошметки тушки сверчка разлетелись по комнате, оставляя на обшарпанных стенах кровавые полосы. К ногам, ошалевшего от грохота и головной боли папы Карло упали вставные челюсти сверчка с прикушенным языком. Джузеппе под шумок опустошал бутылку. Когда контейнер с патронами опустел, Буратино посмотрел на солидный пролом в стене.
- ASTA LA VISTA, BABY! - произнес Буратино и дунул в один из стволов. Взметнувшееся облачко гари осело на его лице.
Буратино развернулся и посмотрел на пьяного Джузеппе, пристававшего к протрезвевшему Карло с просьбой изготовить ему пару таких пугачей. Почувствовав на себе взгляд, Джузеппе съежился от страха и забился под стол. Буратино повесил за спину шарманку и шагнул в пролом.
- Куда он пошел? - спросил Джузеппе.
- Не знаю, - ответил папа Карло, с тоской провожая взглядом удаляющуюся фигуру.
Там, в сумке с инструментами, у него лежала бутылка с отличным самогоном, которую он хранил на непредвиденный случай.
- Не знаю, - повторил он. - Но точно, не в школу...

Завидев издали громадную фигуру Буратино, прохожие щемились в подворотни, так, что улица казалась пустынной. Он направился по главной улице к центру города, где на центральной площади находился всем известный бордель. Бордель принадлежал некому Карабасу-Барабасу, который славился чудовищной силой, необузданным нравом и длинной бородой рыжего цвета. Навигационный компьютер Буратино показывал, что дорога проходит возле школы.
- Эй, дядя, закурить не найдется? - раздался чей-то голос. Скрипя сервомоторами, Буратино повернул голову. Школа представляла собой низкое, серое здание, похожее на барак, с провалившейся крышей и разбитыми окнами. Она производила мрачное впечатление. Не оживляли фасад и многочисленные граффити на стенах. Во дворе тут и там лежали кучи мусора, состоявшие в основном из битых бутылок, шприцев и сигаретных пачек. Несмотря на поздний час, во дворе резвилась детвора. Кое-кто, уже вдоволь нарезвившись, сидел с отрешенным видом и смотрел в одну точку, кое-кто пребывал в отключке. Голос принадлежал прыщавому подростку с подозрительно блестящими глазами, который сжимал в руках бейсбольную биту, утыканную ржавыми гвоздями. Ударная часть была испачкана чем-то красным.
- Ты что - глухой? - переспросил мальчуган. Буратино проанализировал ситуацию и выбрал наиболее подходящий ответ.
- Пошел в жопу!
Нетрезвый подросток, прикинув разницу в весе и размер кирзовых сапог, решил ретироваться.
Возле входа в бордель стояла длинная очередь. Буратино, расталкивая людей, продвигался к входу. Там его остановил вышибала.
- Плати деньги, - рявкнул он, поигрывая электрошокером.
- Нет у меня денег, - огрызнулся Буратино.
- Тогда вали отсюда, - посоветовал охранник.
Толпа позади начала волноваться.
- А ты у меня азбуку купи, предложил Буратино, вплотную приблизившись к вышибале. Охранник ткнул электрошокером в корпус и нажал кнопку. Яркая вспышка разряда вывела из строя прибор, залив расплавленным пластиком руку незадачливого вышибалы. Тот взвизгнул от боли, но пудовый кулак монстра положил конец его мучениям. Буратино беспрепятственно вошел в зал. Веселье было в полном разгаре. Накачанные спиртным посетители отплясывали под вспышки стробоскопов. На подиуме крутилась лучшая стриптизерша Карабаса - Мальвина. Толпу напирающих почитателей с мрачным видом сдерживал телохранитель Мальвины Артемон. Артемон был результатом генетического эксперимента, в результате которого появился этот наполовину человек, наполовину пес. Вид у него был угрожающим, поэтому почитатели, несмотря на принятую на грудь дозу, молча переносили тычки в зубы и удары.
Буратино оценил обстановку и двинулся к сцене. На пути вырос кокой-то субъект в дурацкой шапочке.
- Слышь, кореш, я смотрю, ты тут новенький, экстази не желаешь? Первоклассная штука! У кого угодно спроси, скажут, что у Арлекина лучшие колеса в этой дыре. Буратино продолжал не спеша двигаться дальше.
В это время, прорвавшись через оцепление, на сцену выскочил человек, одетый как хиппи. Длинные рукава волочились по полу, за спиной болталась гитара.
- Мальвина, любовь моя, - завопил хиппи ломающимся голосом, бросаясь на колени перед обнаженной красоткой. При этом гитара больно стукнула его по затылку. Не обращая внимания на боль, хиппи продолжал вопить фальцетом.
- Я написал песню, которую посвятил тебе. Я хочу ее исполнить.
Перекрутившийся ремень гитары начал душить своего владельца. Хиппи попытался снять гитару, но тщетно.
- Пьеро, какого черта ты тут делаешь,- прошипела сквозь стиснутые зубы Мальвина, не забывая при этом улыбаться зрителям. - Ты же обещал мне не прикасаться больше к наркотикам.
Обкуренный Пьеро отчаянно боролся с ремнем, который уже успел опутать ему руки, и не слышал Мальвину. Около сцены, зажимая окровавленный нос, появился Арлекин.
- Эй, ты, - прогундосил он Пьеро, - ты мне с прошлой недели должен.
Завязалась потасовка, в которую была втянута Мальвина. Посетители, побросав все свои дела, ломанулись к сцене. Артемон, увидев это безобразие, рванулся туда же. Началась всеобщая свалка, посреди которой невозмутимо возвышался Буратино. Из состояния невозмутимости его вывел прилетевший неизвестно откуда стул, который разбился о его голову. Буратино воспринял это как личное оскорбление. Поправив сползший колпак, он стянул с плеча шарманку и, направив ее в потолок, дал длинную очередь. Через мгновение на его голову обрушилась массивная люстра. Для Буратино все погрузилось во мрак.



X-PUZZLE

Иван Скляров (Sklyarov@real.xakep.ru)

«ПРОЙДИСЬ ДЕБАГГЕРОМ ПО СВОИМ МОЗГАМ!»

Не стесняйся присылать мне свои ответы, даже если ты смог ответить всего на один пазл, я с интересом почитаю твои оригинальные решения. Ну, а имена героев, которые первыми правильно ответят на все вопросы, конечно же, будут опубликованы в журнале, чем прославятся на всю Россию (и не только) и навечно войдут в историю X. Приз за нами не заржавеет. ;)
Но помни: в большинстве случаев вариант ответа засчитывается как правильный, только если к нему приложено подробное и ВЕРНОЕ объяснение, почему выбран именно этот вариант, а не какой-либо другой.

ОТВЕТЫ К ПРЕДЫДУЩЕМУ ВЫПУСКУ X-PUZZLE

ОТВЕТ НА ПАЗЛ №1 «gcc vs g++»

По умолчанию компилятор gcc не подключает стандартную библиотеку языка C++ libstdc++, поэтому при компилировании программы на языке C++ ее нужно указывать явно с помощью ключа -l, т. е. следующая командная строка откомпилирует программу: gcc hello.cpp -o hello -lstdc++.

ОТВЕТ НА ПАЗЛ №2 «Исправь баги»

В первом листинге кода содержится ошибка Integer Overflow, заключающаяся в том, что если ввести число >= 2147483648, то программа вместо прибавления денег к бюджету будет их вычитать. :) Для устранения этого бага, достаточно добавить ограничение на максимальный размер вводимых чисел, т. е. нужно переписать строку с условием, например, так: if (rub<0 || rub>214748364)

Второй кусок кода подвержен ошибке Buffer Overflow. Для устранения достаточно добавить ограничение на количество вводимых чисел:
for (i=0; (buff[i] = getchar())!=EOF && i<100; ++i)

В третьем куске возможна ошибка Heap Overflow. Чтобы избавиться от этого бага необходимо заменить функцию strcpy на strncpy:
strncpy(one, argv[1], 100)

Четвертая программа подвержена ошибке Format String. Чтобы устранить эту ошибку необходимо добавить спецификатор формата:
fprintf(stderr, "%s", argv[i]);

ОТВЕТ НА ПАЗЛ №3 «CRYPTFUCK v2.1»

CryptFuck v2.1 мог зашифровать слово "Ash" так: 310113163131501. Алгоритм шифрования работает по следующему принципу. Каждое значение ASCII-кода символа переводится в восьмеричное значение, а затем справа и слева к полученному значению подставляются случайные числа в диапазоне от 0 до 9.
Процедура, реализующая данный алгоритм на языке C++ имеет следующий вид:

```
void printChar(char *nPtr)
{
for (; *nPtr != '\0'; nPtr++) {
srand(time(NULL));

cout << rand()%9;
cout << oct << int(*nPtr);
cout << dec << rand()%9; }
}
```

ОТВЕТ НА ПАЗЛ №4 «Пропускная система»

Если наложить все экраны друг на друга то останется незаполненным одно поле, его и нужно нажать.

«ШЕСТЬ ЗАДАЧ С ИЗЮМИНКОЙ»

Попробуй ответить на пять маленьких задачек с изюминкой, но не забывай, ответ засчитывается как правильный, только если к нему приложено верное объяснение.

Первая изюминка

Какое расстояние для фидошника меньше: от 5020 до 5045 или от 5020 до 5080?

Вторая изюминка

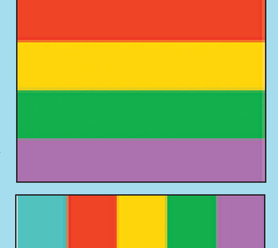
С каким известным языком программирования может ассоциироваться "мертвый страус"?

Третья изюминка

Если пропускная способность канала 64 Мбит/с, то за какое время по нему будет скачан 64МБ файл? Примечания: Считается, что канал качает в полную силу. Ответ нужно указать до долей секунды.

Четвертая изюминка

Какой из приведенных рисунков GIF (правый или левый) поместит на странице хороший Web-дизайнер, если в визуальном плане выбор равноценен?





(О причинах того, стоит ли вообще помещать подобные рисунки на Web-страницу задумываться не будем. :))

Пятая изюминка

Какой протокол лишний в списке: HTTP, SSH, POP3, FTP?

Шестая изюминка

Каталог /tmp в Linux содержит 3 подкаталога. Какое минимальное число ссылок должно иметься на него? Не забывай про вопрос "почему?" ;).

LAMAРАЗМЫ

Иногда наши авторы выдают такие шедевры, что Жванецкий должен повеситься на своих подтяжках

- но так, чтобы он не догадался о твоем причастии к этим проделкам.
- проще говоря, за небольшую плату они перестают трепать языком общественности.
- Загвостка крионики в том,
- "FBI ownz you, Fluffi Bunni" - с интонацией произнес сотрудник спецслужб
- время неумолкаемого роста инета
- что сделать непросто, учитывая учитывать неоправданную уверенность админов в том, что проблема скрывается в чем-то другом.
- Большинство времени (в идеале) ядро ничего не делает.
- Ими я активно пользуюсь, так что тебе советую того же.
- формализовать которые не порой могут даже лучшие эксперты в данной предметной области.
- Через некоторое время, удовлетворительно хмыкнув,

4 приз



Годовая подписка на журнал Хакер

И последний приз забирает некто LasTNighT (last-night@mtu-net.ru), письмо с ответами, от которого, я получил вечером 31 числа.

3 приз



Элитный коврик Хакер WELCOME и годовая подписка на журнал Хакер

Как ни горько в этом признаваться, но с крутым ковриком придется растаться в пользу bool (sunduk@mail333.com). Заслужил! :)

«NMAP ДЛЯ ЛАМЕРА»

Ниже приведены три случая сканирования удаленного хоста в Интернет. Посмотри внимательно и объясни, почему ни один из случаев не возможен в реальной жизни. Сканирование осуществляется с помощью программы nmap (версия значения не имеет).
Считается, что админы хостов полные дятлы, и не предприняли СОВЕРШЕННО ни каких мер по запудриванию мозгов хакерам (эмуляторы также отсутствуют). Также известно, что на всех узлах работают стандартные службы (на стандартных портах).
Доменные имена www.example1.com, www.example2.com и www.example3.com вымышлены.

■ Случай первый

```
[root@server /root]# nmap -sS -O -P0
www.example1.com
Starting nmap V. 3.00 (www.insecure.org/nmap/)
Interesting ports on www.example1.com
(192.168.200.10):

(The 1018 ports scanned but not shown below are in
state: closed)
Port      State     Service
21/tcp    open      ftp
22/tcp    open      ssh
25/tcp    open      smtp
80/tcp    open      http
110/tcp   open      pop-3
143/tcp   open      imap2

Remote operating system guess:
Linux 2.2.12 - 2.2.19

Nmap run completed -- 1 IP address (1 host up)
scanned in 501 seconds
```

■ Случай второй

```
[root@server /root]# nmap -sS -O -P0 -p 1-65535
www.example2.com
Starting nmap V. 3.00 (www.insecure.org/nmap/)
Interesting ports on www.example2.com
(197.85.13.105):

(The 65530 ports scanned but not shown below are in
state: closed)
Port      State     Service

22/tcp    open      ssh
25/tcp    open      smtp
80/tcp    open      http
514/tcp   open      syslog
3306/tcp  open      mysql

Remote operating system guess:
Linux 2.14.16 - 2.4.18

Nmap run completed -- 1 IP address (1 host up)
scanned in 950 seconds
```

■ Случай третий

```
[root@server /root]# nmap -sS -O -P0 -p 1-65535
www.example3.com
Starting nmap V. 3.00 (www.insecure.org/nmap/)
Interesting ports on www.example3.com
(129.123.10.117):

(The 65528 ports scanned but not shown below» are in
state: closed)
Port      State     Service
22/tcp    open      ssh
80/tcp    open      http
25/tcp    open      smtp
139/tcp   open      netbios-ssn
143/tcp   open      imap2
901/tcp   open      samba-swat
1433/tcp  open      ms-sql

Remote operating system guess:
Windows 2000 Advanced Server

Nmap run completed -- 1 IP address (1 host up)
scanned in 1012 seconds
```



Мега-папская куртка FBI, футболка HACK OFF и годовая подписка на журнал Хакер

В прошлый раз пришло всего около двух десятков писем с ответами, вместо обычных пары сотен. :) Видимо сказалась сложность вопросов, зато ответы были такие, что я долго разрывался кому отдать призы. Думаю, в этом выпуске, можно немного расслабиться. ;)
А первый приз забирает gamerX (gamerx@inbox.ru). Все ответы были идеально правильными. Супер! Поздравляем!



Стильная футболка HACK OFF и годовая подписка на журнал Хакер

А вот такие письма я периодически получаю от победителей X-Puzzle: «Моё состояние, когда я увидел себя среди победителей, причём на 1 месте, невозможно описать. Я стоял в метро, втыкал в журнал минут 5, потом начал озираться по сторонам с такой улыбкой, что люди пугались. Потом была моя станция, я пропрыгал по вагону, поцеловал какую-то девушку, получил по лицу и отправился по своим делам немного отрезвлённый (всё-таки неплохие удары у девушек %))». А одна победительница, например, написала, что в день, когда она стала победительницей, переспала сразу с четырьмя мужиками (!), поставив тем самым личный рекорд. Мы всегда рады дарить счастье нашим читателям. ;)
Короче, второй приз уходит к www-www. По его же просьбе, мыло не сообщаю. Черт возьми, www-www, заведи себе дополнительное мыло на халявном хостинге – девушки желают познакомиться.

Правильные ответы читай в следующем номере. Если хочешь получить приз, присылай свои ответы до 1 июля. До встречи!

Юниты

Борда

Мессадж можно закинуть на
board@real.xakep.ru





Объявления рекламного характера не публикуются!

1. мы не будем рекламировать твою страничку, сервер и прочее
2. все письма с матом и прочей шнягой удаляются сразу
3. мы постараемся размещать сообщения в ближайших номерах, но ничего не обещаем :)

OK





Разработаю сайт за веб монеты или нал. Первому бесплатно. Нашампунивать на anonymnos@mail.ru

С радостью приму на себя тяжелую ношу модерирования какого-либо компьютерно-хакерского форума. Имеется опыт сидения, общения и т.д. в форумах. А также есть куча новых идей по улучшению обстановки в форумах (Уменьшение флейма и флуда). Предложения мыльте на: t.j.e_mail@rambler.ru в subject'е ставьте "board"

Продаются:Журналы "Хакер"с 37 по 42 2002 года. Отдаю 6 по цене 5. В отличном состоянии. Мылить на Death@list.ru







Студии Web-дизайна требуются молодые специалисты всех областей, которые готовы долго и плодотворно работать в коллективе единомышленников www@hi-grace.ru

Хороший программист на Delphi ищет хорошую хак-группу. Могу написать любую ХАК-прогу не более 400кб мыльте сюда:Cruk1@yandex.ru





Все программисты желающие поучаствовать во взломе, пишите на мыло hardy87@bk.ru Расскажу подробности и т.д. Если вы разбираетесь в C++, Perl, Html, PHP, JavaScript то вы 100% подходите нам.



Продаю скрипт интернет рассылки! Не требуется sendmail и т.п. Всего за 2$. И скрипт интернет пирамиды за 4 $. Или поменяю это на что-нибудь полезное. Shiva [shiva@xaker.ru]



Перцы, ищу инфу по созданию демок. Также вступлю какую-нибудь кодерскую комманду. Юзаю Delphi. Ваши предложения жду на мыло: qnx_4ever@bk.ru

Продам дистрибутив ASP Linux за 500р.(договорная) Куплю спец по web, linux, Hi-tech. Михаил Барков [geek@bk.ru]

Выполню заказы по 3D моделированию. Рассмотрю любые интересные предложения. Исполнение by hand!!! FOR FREE!!! Mike [d3b1g@mail.ru]





Девушка 16 лет ищет хакера с компом для совместного взлома. (интим по обстоятельствам :) Даша [tagra@ok.ru]







Нам необходимы люди которые готовы потратить некоторое время на то, чтобы донести информацию до тех, кому она нужна, заключается это в том чтобы вы время от времени посылали нам новости, мысли, предложения, или помогали бы проекту каким-либо другим способом. http://linux.iphosting.ru Jakutju[подобный_пустоте] [gipoz@bk.ru]

Продаю порно сайт за 300 WM. Мылить на vasyazaycev@rambler.ru



ХАКЕР VER 06.03 (54)